UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON AT SEATTLE

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	CASE NO. CR19-00159-RSL
	)	
v.	)	Seattle, Washington
	)	
PAIGE A. THOMPSON,	)	June 9, 2022
	)	9:00 a.m.
Defendant.	)	
	)	JURY TRIAL, Vol. 3 of 9

VERBATIM REPORT OF PROCEEDINGS
BEFORE THE HONORABLE ROBERT S. LASNIK
UNITED STATES DISTRICT JUDGE

APPEARANCES:

For the Plaintiff:

ANDREW C. FRIEDMAN
JESSICA M. MANCA
TANIA M. CULBERTSON
United States Attorney's Office
700 Stewart Street, Suite 5220
Seattle, WA 98101

For the Defendant:

MOHAMMAD ALI HAMOUDI
NANCY TENNEY
Federal Public Defender's Office
1601 5th Avenue, Suite 700
Seattle, WA 98101

BRIAN E. KLEIN
MELISSA A. MEISTER
Waymaker LLP
515 S Flower Street, Suite 3500
Los Angeles, CA 90071

Reported by:

Nancy Bauer and Marci Chatelain
Official Federal Court Reporters
700 Stewart Street, Suite 17205
Seattle, WA 98101

INDEX

GOVERNMENT EXHIBITS

EXHIBIT	ADMITTED	WITHDRAWN
111	18	
205	25	
206	16	
207	35	
210	43	
251 and 252	147	
301	133	
302	134	
303	134	
304	135	
305	135	
306	136	
307	140	
308	138	
309	138	
310	139	
401	148	
402	115	
403	148	
404	115	

GOVERNMENT EXHIBITS

EXHIBIT	ADMITTED	WITHDRAWN
405	148	
406	115	
407	148	
408	115	
409	148	
410	115	
411	115	
412	148	
413	115	
414	115	
415	148	
416	115	
417	148	
418	115	
419	115	
420	148	
431	151	
433	151	
434	151	
435	151	
436	151	
437	112	
438	151	

GOVERNMENT EXHIBITS

EXHIBIT	ADMITTED	WITHDRAWN
439	151	
450-462	117	
501 through 506	164	
521 to 525	156	
711	59	
712	60	
713	62	

DEFENSE EXHIBITS

EXHIBITS	ADMITTED	WITHDRAWN
1008	96	
1009	94	
1013	106	

PROCEEDINGS

THE FOLLOWING PROCEEDINGS WERE HELD
IN THE PRESENCE OF THE JURY:

THE COURT: So we still have Mr. Fisk up here, formerly from Capital One, now with Meta, and Andrew Friedman is doing the direct examination.

MICHAEL FISK,
having been previously sworn, testified as follows:

DIRECT EXAMINATION continued
BY MR. FRIEDMAN:

Q. When did Capital One first receive what they recognized as notice of this breach?

A. We received the tip on July 17th, 2019.

Q. And do you recall in what form you received that tip?

A. Yes. It was an email from Kat Valentine.

Q. Would you take a look at Exhibit 201 and tell me if you recognize that?

A. Yes, that's the email.

Q. When did you learn about this email?

A. I learned on the morning of the 18th, in the morning standup.

Q. What is a "morning standup"?

A. It's where the security team gets together every morning to discuss any sort of hot topics.

Q. And in terms of your work schedule, once you learned about this, what impact did it have on you?

A. I told my admin to clear my calendar and that I was going down to the operations center.

Q. Was that something that happened broadly within the Cyber Organization?

A. There was already a fair number of folks from our operations and intelligence team that were down there, but, yeah, a few of us, like me, also joined them that morning.

Q. In general terms, when Capital One, or maybe any company, receives an alert that appears to be real, are there a series of goals or steps that you're trying to take?

A. Yes. The first thing you want to do is just confirm the veracity. Can we tell what the vulnerability was, for example, that's being leveraged here, and can we close the vulnerability, is the first thing.

Q. What is the second thing?

A. You want to understand, you know, was there a successful compromise, you know; just understand if this -- you know, the tip reported, you know, one compromise, but has the same thing been used before or after.

Q. And if you confirm that, what's the next step that you take?

A. You want to understand the extent of -- was any information taken, was there any damage done, and what is the extent of that.

Q. Before you fully understand the extent of the damage, are there other things you want to do?

A. Like I said, when you find the vulnerability, you definitely want to close that, is the first thing that you do.

Q. Okay. Got it. And then full analysis and understanding after that?

A. Yeah.

Q. Did Capital One, basically, follow that set of steps or procedures in addressing this?

A. Yes.

Q. In order to understand the vulnerability, what was the first thing Capital One did?

A. Well, in this case, we were provided with, you know, a command line that purported to give access, and so it was reasonably straightforward to try to reproduce that, you know, same action, and confirm that it worked.

Q. Did you go to the link?

A. Yes.

Q. Okay. And this is on a particular website; is that correct?

A. Yes.

Q. What is that website?

A. The site is called GitHub.

Q. And what is GitHub?

A. It's primarily a source code repository site that's used for open-source projects. Basically, it's a place where computer programmers store computer code.

Q. Is it supposed to be collaborative or sharing?

A. Most -- a lot of what's on there is open to the world intentionally, yes.

Q. In what form do you put information on GitHub?

A. There's multiple forums. Some is sourcebit files, and then relevant to this, there is another thing that they call a gist, g-i-s-t, pronounced "*jist*."

Q. What is that?

A. It's sort of a scratch pad, text file, sort of open note-taking mechanism. It's a place to post freeform text.

Q. Are gists public or private?

A. I think they can be either. This one was public.

Q. But would you know -- it has a complicated -- the link is not easily memorizable; it is not your dog's name?

A. Yes. In this case, there was a direct link to it that gave us access.

Q. If you didn't have that link, is there an easier, obvious way to get there?

A. You can search for gists as well.

Q. Would you have to know what you were searching for, though?

A. Yes.

Q. When you went to the gist and saw the gist, what was it?

A. It was a command being executed, and then the output of that command.

Q. Okay. And let's look at Exhibit 204.

Is that the gist?

A. Yes.

Q. And if we look at the second page of that, what do you see there?

A. Those are a list of Capital One buckets from AWS, places where data are stored.

Q. Okay. We'll come back to the details of it, but was there also code in this gist?

A. There was command lines that were executed.

Q. And did that contribute to how you tried to replicate the vulnerability?

A. Yes.

Q. Were you able to replicate what those command lines indicated was the vulnerability?

A. Yes.

Q. Once Capital One had confirmed -- did that confirm the vulnerability for you?

A. Yes.

Q. Once Capital One had confirmed that vulnerability, what did it do?

A. We needed to understand what made that command work. We confirmed vulnerability was there, but you need to understand the nature for the vulnerability and how to fix it, and then fix it.

Q. And was Capital One able to do that?

A. Yes.

Q. By when had you confirmed the vulnerability and fixed it?

A. The 18th.

Q. So the day after this email came in?

A. Yes.

Q. And how did Capital One fix the vulnerability?

A. In this case, we -- well, identified that there was a misconfiguration on a WAF, a web application firewall, and we, actually, just replaced that WAF with a new one, which was a project that was under way anyway.

Q. When you say "a new one," is this like my air conditioner gets old and stops working, or is it more complicated than that?

A. I mean, it's software, so it doesn't necessarily stop working like your air conditioner. But it was a different make and model that we had selected and were in the process of rolling out, and so we just went to that upgrade.

Q. More quickly than it would have happened?

A. Yes.

Q. Okay.

In addition to -- we've gone partway through the thing, and stopping this, was Capital One continuing to communicate with Kat Valentine?

A. Yes.

Q. Would you take a look at Exhibit 202 and tell me if you recognize that?

A. Yes.

Q. That's another email from Ms. Valentine?

A. Yes.

Q. When did this one come to Capital One?

A. On the 19th.

Q. Okay. And there are some attachments to it; is that fair to say?

A. Yes.

Q. Did you look at those attachments?

A. Yes.

Q. Would you look at Exhibit 203 and tell me if you recognize that?

A. Yes.

Q. It is a multipage exhibit.

A. Yes.

Q. Were those attached to this email?

A. Yes.

Q. In general terms, what were these attachments?

A. They were, I believe, Twitter posts from the handle Erratic.

Q. Do you recall one of them referring to Capital One?

A. Yes.

Q. Turning to page 5, is this the Twitter post to which you were referring?

A. Yes.

Q. Okay. There seems to be three separate lines or -- probably, perhaps, two posts, but three lines; is that accurate?

A. Yes.

Q. What does the first one -- what's the reference to Capital One there?

A. It's referring to Capital One documents, and stating that they will be dropped.

Q. What are dox, d-o-x?

A. "Documents" is how I interpret that.

Q. Okay. So how do you interpret "Capital One dox"?

A. Documents that belong to Capital One.

Q. And what do you understand "dropping" to mean?

A. Probably making it public.

Q. And then the next line says, "I wanna distribute those buckets first I think"?

A. Yes.

Q. Do you link "buckets" to Capital One dox?

A. Yes.

Q. And can you explain how and why?

A. I interpret "dox" to not, you know, necessarily be just a paper document or a Word document but sort of data in general. And so I interpret that as referring to buckets of Capital One data and potentially releasing them to the public.

Q. And what does the last line, the next Tweet say?

A. Well, it says, "Their SSNs with full name and DOB," which I interpret to mean there are Social Security numbers with full names and date of births.

Q. Was Capital One concerned when it received this attachment?

A. Yes, very.

Q. And why is that?

A. Well, it indicates that there could be an exposure of our customers' private data to the public.

Q. As part of your investigation, was Capital One able to confirm whether data had, in fact, been taken out of Capital One?

A. Yes.

Q. And what was the answer?

A. It was taken, yes.

Q. By when did Capital One confirm that?

A. On the 18th, I believe, we confirmed -- or the 19th, I think, we confirmed that data was successfully taken, and then on the 20th, we had identified that there were things like customer privacy information in the data.

Q. What did Capital One do once it had confirmed that?

A. Well, several things, but one was to notify law enforcement.

Q. Do you recall, generally, what law enforcement you notified?

A. The FBI, I believe.

Q. Okay. By the time that Capital One notified law enforcement on the 20th, did you believe you had identified the person responsible for this?

A. Yes; since the initial tip provided some strong indications, yes.

Q. Let's go to Exhibit 201, and tell me what you're calling an "indication."

A. So the URL, the link there to GitHub, the thing after "GitHub.com" says "Paige Adele Thompson," and then, in GitHub, posts are owned by a user, and that part of that URL is what has the user name for the person who posted the information.

Q. So did you believe it was someone named Paige Adele Thompson?

A. Certainly that was the hypothesis, given the name, yes.

Q. Okay. Did you or people working with you go to linked sites, sites that were linked or connected to this GitHub site?

A. Yes.

Q. Where did you go?

A. One of them was a link to GitLab, which is a similar sort of publishing site.

Q. Okay. And from GitLab, was there anywhere particular that you went?

A. Yeah. On that site, we found a resumé for Paige Thompson.

Q. Would you take a look at Exhibit 206 and tell me if you recognize that?

A. Yes.

Q. Is that the resumé?

A. Yes.

MR. FRIEDMAN: Your Honor, this has not been offered, so government offers Exhibit 206.

MR. HAMOUDI: I don't have an objection.

THE COURT: 206 is admitted and may be displayed.

(Government Exhibit 206 admitted.)

Q. (By Mr. Friedman) Whose resumé is that that you found?

A. Paige Thompson's.

Q. Does it list a variety of jobs?

A. Yes.

Q. What is the most recent job listed?

A. It was with Amazon.

Q. And a specific part of Amazon?

A. It says, "Simple Storage Services," which is part of the AWS cloud service.

Q. Is that S3 when we talk about S3 and S3 buckets?

A. Yes.

Q. When had Ms. Thompson worked at Amazon or AWS?

A. In 2015 and 2016.

Q. And so when you were looking at this, how long since her employment terminated?

A. Well, it was 2019, so it was two and a half, going on three years.

Q. And then above that, do you see the top section that talks, I guess, about skills or proficiencies?

A. Yes.

Q. Let's look at the section related to AWS. What are the first three proficiencies listed there?

A. S3, the Simple Storage Service; EC2, which is the elastic computer virtual server service; and IAM, which is Identity and Access Management service.

Q. Okay. Mr. Fisk, do you have an understanding, from your work with the breach, of how this breach took place?

A. Yes.

Q. And in general terms, did it relate to misconfigurations or configurations of different things at Capital One?

A. Yes.

Q. Were there two principal ones?

A. Yes.

Q. Would looking at Exhibit 111 -- this has not been offered so it will just be on your screen -- would that help explain your understanding?

A. Yes.

MR. FRIEDMAN: Government offers Exhibit 111.

THE COURT: Any objection?

MR. HAMOUDI: No, Your Honor.

THE COURT: It is admitted and can be published.

(Government Exhibit 111 admitted.)

Q. (By Mr. Friedman) Mr. Fisk, this is titled "Web Application Firewall." What is a -- well, let's start with: What's a firewall?

A. A firewall is something that sits in the network and screens traffic going across it and decides to permit traffic that is meant to be delivered to what's behind the firewall and to block traffic that could be malicious traffic or undesired traffic.

Q. And in this case, it says not just firewall but "web application firewall." Why is that?

A. Web application firewall is a type of firewall that focuses on web application. So it looks at web traffic, specifically, and decides to selectively forward web requests.

Q. Okay. So this diagram depicts two things between an external device and the internal server or cloud. Can you tell us what each of those is and what its role is?

A. Yes.

In front of the firewall, as we say, or to the left on the diagram, is a thing called an elastic load balancer, which is another AWS service that is used when you need to support a lot of traffic for a popular site; for example. You actually have more than one internal server, they're identical, and more than one WAF that are identical, and the load balancer just kind of steers traffic evenly to the different WAFs and servers so that they can keep up.

Q. And then behind that, we see the web-facing server and WAF?

A. Yes.

Q. And how does the purpose of that differ from the load balancer?

A. So the load balancer just sort of directs the traffic to the WAF. The WAF makes that filtering/screening decision I described, and then if it permits the traffic, it delivers it to the internal server.

Q. I'm going to ask you to look at Exhibit 107, and this has been admitted. Do you recognize that?

A. Yes.

Q. And does that explain what actually happened in this case?

A. Yes.

Q. Okay. Can you walk me through that, step by step?

A. Yeah. So the firewall here, which is the same as the WAF in the previous picture, is what had the configuration issue, and it allowed a specially formed request from the client, on the left here, to go through the firewall and be proxied or relayed to the Instance Metadata Service on the lower right.

Q. Okay. Can I stop you there for a second and ask, are you familiar with something called a port?

A. Yes.

Q. Is what is a port?

A. So computers are identified on the Internet by IP addresses, and then on an individual computer, you can have multiple ports or services running. And so the port is what lets you direct traffic to a particular piece of software or service on a computer.

Q. Okay. You said you can have multiple ports on an IP address; is that correct?

A. Yes. A computer can be both a web server and an email server, for example.

Q. So how would being both a web server and an email server, how does relate to the concept of ports?

A. So the web server listens on one port; for example, 443 is the port used for encrypted web traffic, customarily. And an email server would listen on port 25, which is the standard port for email delivery.

Q. So the same computer but listening in two different directions or ways?

A. Yes.

Q. How many different ports can there been on a computer?

A. 65,000, roughly.

Q. 64,000 --

A. 64,000, yeah.

Q. All right. In this case, did the misconfiguration relate to a particular port?

A. Yes.

Q. And to which port did it relate?

A. 443.

Q. To your knowledge, were the other ports on this server -- or firewall configured correctly?

A. Yes.

Q. And port 443, I think you said it relates to web traffic. Does it relate to some, or all web traffic?

A. It is the primary port used for encrypted web traffic, so if you ever see "https" in the URL, it's likely going over port 443.

Q. Is there a different port for unencrypted web traffic?

A. Yes. Port DD is the standard port for that.

Q. What was the effect of misconfiguration?

A. The effect was that a specially formed request to the firewall would get proxied or relayed, on the requester's behalf, to a destination of the requester's choosing.

Q. Okay. And in this case, what destination was that?

A. The Instance Metadata Service.

Q. Are external computers supposed to be able to communicate to the Instance Metadata Service?

A. No.

Q. What happened when the communication reached the Instance Metadata Service?

A. It was delivered as a web protocol request, and the Instance Metadata Service responded.

Q. And why did the Instance Metadata Service respond?

A. It viewed the request as coming from the local system, from the firewall, and that is -- the one and only kind of request the Metadata Service will answer to is a request from the local computer.

Q. So it misinterpreted the source of the request?

A. Yes.

Q. Once it did that, what did the Instance Metadata Service do?

A. It fulfilled the request.

Q. Okay. And can you tell us what fulfilling the request meant?

A. Well, in this case, the first request was to return the name of the role being used by the firewall, and so it did.

Q. Okay. And after it did that, what happened next?

A. Well, there was a subsequent request that asked for a copy of the key, the credential used to authenticate that role.

Q. And when that information was returned, first the name of the role and then the credentials, where did those go?

A. Those went back to the client computer, on the left here, under Ms. Thompson's control.

Q. Okay. So that's one configuration, the configuration of the firewall.

To what did the second configuration relate?

A. It relates to what information the key that was stolen had access to.

Q. When you say "key," to what are you referring?

A. The role credential. So the way the computer will identify itself as being the firewall, in this case, is a key or a credential.

Q. To what kind of data does a firewall normally need to have access?

A. It would be to have access to its own configuration information and ability to write logs for what it sees.

Q. Do firewalls generally need access to bank customer credit information?

A. No.

Q. Did this credential have permission to read, at least, some customer and credit information?

A. Yes.

Q. Would you look at Exhibit 108, which has been admitted, and tell me if that helps explain what happened next?

A. Yes.

Q. How is that?

A. So once Ms. Thompson had the key for the WAF and could impersonate the WAF, she could use that key directly to access the AWS S3 service -- AWS makes that service available on the Internet to anyone with the right key -- and could access, and she did access the data directly from S3 at that point.

Q. Okay. I'm going to refer -- the gist that you saw, originally, on the Internet. I'm going to refer to that as the

"April 21 gist," if that's okay.

A. Okay.

Q. Did the April 21 gist contain, in addition to a list of buckets, did it contain code or things created by the execution of code that are consistent with what you just explained?

A. Yes.

Q. So let's go to that, if we could, Exhibit 204.

So this is one version, straight off the web. Have you looked at another version that has slightly larger type and is easier to read?

A. Yeah. This one sort of cuts off the lines at the side, but I've seen the version that has the full text.

Q. And would you look at Exhibit 205, which is not admitted, but is that the other version at which you looked?

A. Yes.

Q. Is the information in here the same as the, I guess, the vast majority of the Exhibit 204?

A. Yes.

Q. Does Exhibit 204 contain one slight additional piece of information?

A. Yeah, it has an additional comment at the end.

THE COURT: You said "204," but you meant 205?

MR. FRIEDMAN: That's quite possible. Thank you, Your Honor.

Q. (By Mr. Friedman) Everything in Exhibit 205 is part of

Exhibit 204?

A. Yes.

MR. FRIEDMAN: The government offers Exhibit 205.

MR. HAMOUDI: No objection.

THE COURT: 205 is admitted.

(Government Exhibit 205 admitted.)

Q. (By Mr. Friedman) Mr. Fisk, I'm going to ask you to relate some of the things in this document to the methodology you just described with those diagrams.

A. Okay.

Q. And if we could focus on the top, say, eight to ten lines.

In the top right-hand corner, do you see a date?

A. Yes.

Q. And can you tell us what that date is that you see?

A. Yeah. The 21st of April 2019.

Q. Okay. And then if we drop down a couple lines to the first full line, there is a line that has the second word "CURL"?

A. Yes.

Q. What does "CURL" mean?

A. CURL is a command line tool that you can use to submit web requests.

Q. And when you say "web requests," what does a "web request" mean?

A. You probably would think of a web browser, where you make a web request. This is a command line tool that lets you sort of do that a little bit more manually. But, basically, submit something to the web server asking it to return something.

Q. The next line starts with the word "proxy."

A. Yes.

Q. And then "https," and then a whole bunch of digits. Can you tell us what -- what does "proxy" mean there, first?

A. Yeah. This is an option in the curl command that says send your traffic through a proxy.

Q. Okay. And does this line tell you where the traffic is going first?

A. Yes. The statement right after "dash, dash, proxy" is the system to be used as the proxy.

Q. Okay. And are you familiar with -- this, basically, the first four numbers there, 35.162.65.136, are you familiar with what that is?

A. Yes.

Q. What is that?

A. That was an IP address that belonged to AWS but was used by Capital One at the time for one of our web applications, and it relayed the load balancer and WAF in front of it.

Q. Okay. And is that the one that has the misconfiguration?

A. Yes.

Q. And then there's a colon and the number 443. What does that mean?

A. That is saying that the proxy is on port 443.

Q. Okay. To use that channel to communicate?

A. Yeah, to use port 443 to talk to the proxy.

Q. So if this command is asking or instructing it to go to that web address at that channel as a proxy, does it say where it wants to go after that?

A. Yeah, that's the line after that.

Q. Can you explain, I guess, the beginning of that line?

A. Yeah. So that line and a little bit of the fourth line is a URL, like you would see in a web browser, that is being requested. In this case, the server that's being accessed is the 169.254.169.254 address.

Q. Do you know what 169.254.169.254 is?

A. Yeah. In an AWS environment, that is how you talk to the Instance Metadata Service.

Q. Okay. Does this command also say or instruct what is to be done when it gets to the Instance Metadata Service?

A. Yes. The rest of the line describes the action being requested.

Q. Okay. Before we go into that: Should an external computer be able to get to the Instance Metadata Service in this way?

A. No.

Q. And why is that?

A. Well, it enables attacks like this, so the Instance Metadata Service only accepts traffic locally, and you work hard to ensure that there is no way to relay traffic to a Metadata

Service.

Q. What command of this code instruct to happen when the traffic gets to the Instance Metadata Service?

A. In this case, it is requesting a copy for the security credential for the ISRM-WAF-Role.

Q. What is the ISRM-WAF-Role?

A. Well, I'll explain the acronym first, I guess.

"ISRM" is the old name for the Cyber Organization at Capital One, Information Security Risk Management team. "WAF," as we've described, is Web Application Firewall. So this is a role that was designed to be used exclusively by the WAFs.

Q. By firewalls?

A. Yes.

Q. Now, can you tell anything from the fact that this command includes the name of that role?

A. Yes. You would need to have done something before this to identify the name of that role.

Q. So already to have internal access?

A. Yes.

Q. Is the name of that role even something that was generally public at the time?

A. No.

Q. And I think you said this command asks for the credentials for that role; is that correct?

A. Yes.

Q. And once it gets those credentials, does it have an instruction for what to do with them?

A. Well, it is sending them to a thing called awssession.sh.

Q. What is awssession.sh?

A. It was a script on Ms. Thompson's computer. It appears to, essentially, log you in, so to speak, with that credential.

Q. But that's computer code or script written by Ms. Thompson?

A. Written by her or obtained by her, yeah.

Q. And when you say it "appears" to do something, what are you drawing that inference on? How are you saying that?

A. Further down in the document, you can see use of that credential.

Q. So you're seeing what happened and saying that must be --

A. Yeah.

Q. -- what it asked to have happen?

A. Inference, yeah.

Q. When you say "further down," are you talking about a section that starts with the word "GET," in capital letters?

A. Yes.

Q. So highlighting that, what is the line that starts with the word "GET"?

A. So this is the CURL tool showing what it's doing, based on the arguments that it was given, the parameters it was given. And so "get" is how an http web protocol, you ask for URL, and then it is requesting that same URL that we saw earlier.

Q. So is it fair to say, sort of, output or an intermediate -- it's a translation of the same request?

A. Yes, it's showing you what's going on behind the scenes to fulfill your request.

Q. How do you know it's asking for the same role and credential information that we saw earlier?

A. Well, so it's got the same IP address for the Instance Metadata Service, and it's asking for the ISRM-WAF-Role.

Q. Okay. Are you able to tell if this request was successful?

A. Yeah. In the second half of the highlighted part, where the line starts with "http" but then ends in "200 OK" means there was not an error, and the server responded to the request.

Q. And then do we need to go to the next page to see what happened when it responded?

A. Yes.

Q. Going to page 2, and we'll highlight the top third.

What do you see here that tells you what happened?

A. Well, so here I see a list-buckets command being issued to the S3 service in this "aws s3api" line.

Q. So how is this list-buckets command being issued?

A. It was probably typed by Ms. Thompson.

Q. Can you tell if it's manual or part of that pause-session script?

A. I can't really tell if it was part of the script or manual.

Q. But somehow typed or coming from Ms. Thompson?

A. Yes.

Q. What is "list-buckets"? What is that command? What is it asking someone to do?

A. So it is an AWS command that, for the credential that you have, will return the set of storage buckets that that credential can see.

Q. Sort of like a file directory of what it can see?

A. Yeah.

Q. And what happened when that command was issued?

A. It returned a long list of buckets.

Q. Do we see the first three of those here?

A. Yes.

Q. And do you recognize those buckets?

A. Yes. These are Capital One buckets.

Q. Okay. Everything we've just looked at, the code, all relates to something that took place on one day; is that correct?

A. Yes.

Q. And what day is that?

A. The 21st.

Q. Of April?

A. Of April, yeah.

Q. Okay. Did the attack in this case take place just on one day, or did it span a longer period of time?

A. It spanned a longer period.

Q. For how long did it continue, that you can tell?

A. We saw activity from March through May.

Q. Of 2019?

A. Yes.

Q. How did you see activity? Where did you look to see that?

A. In our event logs that we record.

Q. And when you say "event logs," are you familiar with the term "CloudTrail logs"?

A. Yes.

Q. What are CloudTrail logs?

A. CloudTrail is an AWS logging service where they log a lot of events for things that take place in AWS.

Q. Okay. And do these logs show the commands that are issued, or do they show what happens based on those commands?

A. They show the -- not necessarily the command line that someone types or that initiates the request, but they log the actual requests made to the AWS service, which sometimes match one for one, and sometimes one command may result in multiple events that are logged.

Q. Okay. So it's not what -- if we think really old-school and typing, it's not what was typed, necessarily; it's something a little downstream of that?

A. Correct.

Q. Does Capital One receive a large number of lines of logs per day?

A. Yes.

Q. In the millions?

A. At least.

Q. How did you decide what logs to look at?

A. We had several indicators that we searched our logs for based on the information we had in the investigation, so we certainly had the ISRM-WAF-Role indication, and so one of the things we looked for was everything involving that role.

Q. Okay. And did you look across all your accounts, or at particular accounts?

A. We looked across everything.

Q. Were there other indicators you used to narrow the search of what you were looking for?

A. Yeah. We could see IP addresses that traffic was originating from for this activity, and so we also looked for additional traffic -- any additional traffic from those IP addresses, and there were some other indicators in the traffic, and we used those as well.

Q. Is the other indicator something called "a user agent string"?

A. Yes.

Q. What is a user agent string?

A. So in client-server communications, it's customary to have a field called a "user agent" that is submitted with a request that describes the kind of software you're using. So if you're using your normal Chrome web browser, it would say something that identified what version of Chrome you had, maybe what kind of computer you had; just a bunch of details about the client making the request.

Q. Is it a little like a fingerprint for a computer?

A. It can be, yeah.

Q. More or less accurate, depending upon of what you think of this and what you think of fingerprints?

A. Yes.

Q. Some form of identifier?

A. Yes.

Q. When you looked at the ISRM-WAF-Role and you looked for particular IP addresses and you looked for User-Agent strings, how big of a universe were you able to narrow -- how much were you able to narrow down what you believed were relevant logs?

A. In the CloudTrail logs, there were around 60 entries that matched.

MR. FRIEDMAN: Your Honor, we're about to introduce an exhibit that, if I could turn off the computer for the gallery, if that's okay? We're going to file it redacted, ultimately.

THE COURT: Yes. The government has permission from the court for this exhibit to not be displayed to the public, and with agreement of defense.

Go ahead.

MR. FRIEDMAN: Thank you, Your Honor.

Q. (By Mr. Friedman) Would you look at Exhibit 207, and tell me if you recognize that.

A. Yes.

Q. Do you recognize that?

A. Yes.

Q. Is that the smaller set of, I guess, roughly, 60 lines of logs that we just talked about?

A. Yes.

MR. FRIEDMAN: The government offers Exhibit 207.

MR. HAMOUDI: No objection.

THE COURT: 207 is admitted into evidence.

(Government Exhibit 207 admitted.)

Q. (By Mr. Friedman) Mr. Fisk, if we could go over -- first off, how long -- can you look at how many lines there are in this spreadsheet? How many lines do you see?

A. There are 60 rows, including the header, so 59 log entries.

Q. Fifty-nine lines of data?

A. Yes.

Q. And if we go back to the top and move over to the right, do you see column N?

A. Yes.

Q. What is column N?

A. It is source IP address, so the IP address on the Internet that issued the request to AWS.

Q. Is that one of the pieces of data that you looked at in identifying the relevant lines?

A. Yes.

Q. And when we look down, the first ten or fifteen, there seems to be some variation?

A. Yes.

Q. Do you see where we start to see the name number on every line?

A. Yeah, the "46" addresses.

Q. Do you have an idea what the address starting with 46 is?

A. I believe that was owned by a VPN service in Europe, iPredator, I think.

Q. A virtual private network?

A. Yes.

Q. And then two columns to the right, there's a column labeled "user agent."

A. Yes.

Q. Do you recognize that?

A. Yes.

Q. Okay. Without going into detail, in general, what is the information on each line?

A. It's describing the client being used, the AWS command line interface and the specific major and minor version for that client, and then some things about where that client was built or is running; things about what kind of Linux computer it was, for example.

Q. And was that one of the things you also looked at in terms of narrowing the pool to relevant lines?

A. Yes.

Q. Okay. Although you approached this in that way of, you know, applying these different streams to get to here, kind of, just general confirmation, was there an easy double-check that said, Yep, we've got the right lines?

A. Well, we found lines that matched the information provided on GitHub.

Q. More generally, were there other lines in your logs where this role was being used externally -- by an external user to execute commands?

A. No. This was the entirety of the external use of that role.

Q. Okay. And so your search, that kind of double-check, did that contribute to you thinking, Okay, we've got the right lines?

A. Yes. Part of the investigation was to see if any other roles were used, but we didn't identify any others. So this was the full set, all had the same role.

Q. And so what does this universe of lines from the logs reflect?

A. It is a series of activities over that March through May time period, and requests made using the stolen WAF identity.

Q. Okay. And if we go back to column A, let's get the first page and then the second page.

What is the date range for this group of 59 events?

A. At the top, it starts on March 12th of 2019, and ends on May 26th of 2019.

Q. Is that why you say the conduct of the attack continued for two and a half months?

A. Yes.

Q. If we could go up to the first line, there's a column, column K, towards the right, labeled "event name." What was that column?

A. This is the request that was made to the AWS service.

Q. Okay. And so what does -- the first request says "describe instance," correct?

A. Yes.

Q. What is "describe instance" -- what does that command ask for?

A. It's just asking for some information about an AWS resource.

Q. Okay. Could you issue that command without knowing the name of the resource already?

A. I don't think so, no.

Q. So this line happened on March 12th. What does that tell you about the date that Ms. Thompson first obtained access to AWS computers?

A. Well, it was at least this day, if not earlier.

Q. And then are you aware if this particular command succeeded?

A. I think if you scroll to the right, you can see an error column that will tell you whether or not it succeeded, and this one did not.

Q. Why do you say that?

A. In the error message column, you can see the response, "You are not authorized to perform this operation."

Q. When you say that was the response, was that a response that would have been sent to Ms. Thompson?

A. Yes.

Q. So she would have received that text saying, "You are not authorized"?

A. I believe so.

Q. If we go back to column Q and scroll down, are you able to tell from that whether the majority of the commands that Ms. Thompson entered failed or succeeded?

A. Yes. It looks like the majority failed.

Q. And I see the message, "You are not authorized to perform this operation," in a lot of these rows.

A. Yes.

Q. Are there some rows, specifically, the bottom one, and then the rows that follow, that have slightly different text?

A. Yes.

Q. Scrolling to the right, what is that text?

A. Well, rows 48 through 53 is just a different form of not-authorized message.

Q. Okay. And would that be text that would have gone to Ms. Thompson?

A. I believe so.

Q. Okay. The language that this role is not authorized to perform whatever the command is?

A. Yeah. That's meant to be an error message delivered to the user.

Q. Can we go back and look at the dates in column A, and I want to focus on the period from March 22nd to March 23rd. There should be ten rows.

Do you see that list of ten rows that took place between March 22nd and March 23rd?

A. Yes.

Q. What commands was Ms. Thompson issuing during that period?

A. Get caller identity, describe instance, several list-bucket commands.

Q. What does "get caller identity" ask a computer to do?

A. It tells you the name that corresponds to the credential that you have, sort of a who-am-I command.

Q. Okay. Is that information as having the ability -- let's go to the right and see if those commands succeeded.

A. The lack of an error message tells me the get caller identity, for example, succeeded.

Q. Would that be enough information that Capital One would be interested in having a responsible disclosure, that someone had been able to do this and get this information?

A. Yes. Just getting a credential stolen outside of our environment alone would be definitely something that we'd want to know about and act on.

Q. Did Capital One receive a reasonable disclosure about this in March of 2019?

A. No.

Q. The other commands here listed in that two-day window are list-buckets primarily; is that correct?

A. Yes.

Q. And what does list-buckets do, again?

A. This corresponds to things like we saw before, where it will just return a list of the Capital One buckets that can be seen by that role and credential.

Q. And did those commands succeed?

A. Yes.

Q. Now, does Capital One have other logs that tell what was going on during this period, things that are not reflected in this particular chart?

A. Yes. There's a second type of log that AWS provides that's higher in volume, and so it's provided separately, called "CloudTrail data event logs," and we used those in the investigation as well.

Q. Did you look at the CloudTrail data event logs for March 22nd and 23rd?

A. Yes.

Q. And what did you see, in general terms, when you looked at that?

A. A lot of successful and unsuccessful requests to get files, "GetObject" is the actual "Get" name, essentially, to download a file.

Q. Okay. And would you take a look at Exhibit 210, and tell me if you recognize that.

THE COURT: We're now back on published.

MR. FRIEDMAN: We're going to go back to this in a moment.

THE COURT: So Ms. Manca just is wanting to parade back and forth.

MR. FRIEDMAN: Exercise.

Q. (By Mr. Friedman) Do you recognize Exhibit 210?

A. Yes.

Q. What is Exhibit 210?

A. It is a tally of those log events. Like I said, they were quite numerous, and this is a tally of a number of requests and the time durations for those requests for all the different buckets that were accessed or attempted to be accessed.

Q. During this two-day window?

A. Right.

Q. You said this is a tally. Would the actual logs be voluminous?

A. Yeah. I think there were millions of rows.

Q. Okay. So it would be a multimillion-row spreadsheet?

A. Yes.

MR. FRIEDMAN: The government offers Exhibit 210.

MR. HAMOUDI: No objection.

THE COURT: 210 is admitted.

(Government Exhibit 210 admitted.)

Q. (By Mr. Friedman) Mr. Fisk, is it fair to say there are four tabs in this exhibit?

A. Well, I see three.

Q. There you go.

So I'm going to start with one that says, "Successful list objects requests."

What is a list object request?

A. It just enumerates the objects or files in a bucket; sort of like looking at a folder on your computer and seeing what the names are.

Q. Is this related to the activity we saw in the CloudTrail event logs, the previous exhibit?

A. Yes.

Q. Okay. And can you tell how many -- in general terms, what's the volume of successful requests to list objects during that two-day time?

A. Yeah, I mean, basically, if you're looking at the first column and adding it up, I think it's in the thousands of successful requests.

Q. Okay. And then if we look at the second column, is that a measure of the volume of data for those requests?

A. For the requests. This is just -- this is the link of all the file names put together sort of thing.

Q. And if we go to the "successful get-objects requests" tab, what's the difference between that and the "list objects" tab?

A. So "list objects" is just sort of showing you that list of files in the directory. "GetObject" is actually downloading a copy of a file object.

Q. Can you tell the volume of successful requests here?

A. I recall, if you total it all up, it was between two and three million, I think.

Q. So two or three million files or folders or whatever the objects were?

A. Yes.

Q. There are also two tabs that say "failed list objects" and "failed get-object requests." What are those?

A. Those were similar requests but ones that were unsuccessful due to access controls.

Q. When you say "access controls," what do you mean in this context?

A. So the role credential that we've been discussing, the

ISRM-WAF-Role, did have access to some customer data in this account, but it didn't have access to all of the files, so many of these requests were denied.

Q. So a mix; some succeeded, some failed?

A. Correct.

Q. And this spreadsheet talks about GetObject and list object requests.

A. Yes.

Q. Is that the command that Ms. Thompson would have typed in order to generate this, or would she have typed a different command?

A. She could have done it either way, but there is a sync command that would do that that we saw in one of the gists.

Q. Do you infer anything from the fact that there are millions of these?

A. Probably not something you type by hand.

Q. And the sync command, let's go to Exhibit 204, page 47.

This looks like a comment by Paige Adele Thompson; is that correct?

A. Yes.

Q. And what do you see at the end of that comment?

A. An AWS sync command.

Q. Is that a command that would have generated the get-object and list-object commands that we just saw reflected in the logs?

A. Yes.

Q. So Capital One observed data exfiltration on two days; is that correct?

A. The 22nd and 23rd.

Q. Of March?

A. Yes.

Q. Did it observe other activity after that?

A. Yes, not exfiltration, but other activity.

Q. And if we could go back to Exhibit 207.

MR. FRIEDMAN: Special Agent, can we highlight lines 15 to 38?

Q. (By Mr. Friedman) Do you see activity on a particular date here?

A. Yes, the April 19th.

Q. Okay. And when we go over to the column "event name," towards the right --

A. Uh-huh.

Q. -- that starts with a new command that we haven't talked about, "create keypair."

A. Yeah.

Q. What is a keypair?

A. A keypair is a set of credentials that let you log-in to a computer resource in AWS.

Q. And why is it called a keypair?

A. It uses a form of cryptography called "public private keys," where you -- there are two keys; one is a secret key that is held by the user of the key, and then a corresponding public key that is put on the server that you would access, and the server uses the public key to identify that the person making the request holds the secret key.

Q. And so it allows access?

A. Yes.

Q. Is it a type of credential, even?

A. Yes.

Q. Have you ever heard the term "back door"?

A. Yes.

Q. And what is a back door to you?

A. A back door is something an intruder will create to provide an alternate and longer-lasting form of access should their initial way that they got in stop working or potentially be too noisy and too likely to be detected.

Q. Is creating a keypair a way of creating a back door?

A. Yes.

Q. Are you aware of whether these commands were successful?

A. I believe they were not.

Q. Okay. And let's go to the right and look at the output. What was returned when these commands were entered?

A. "You are not authorized to perform this action."

Q. And that would have been a message sent to Ms. Thompson?

A. Should have been, yes.

Q. And then if we look under there, it looks like "create keypairs," then there are five commands that say "describe keypairs." What does that command do?

A. Well, "create" will create new ones, and "describe" will describe any that already exist.

Q. Why would keypairs already exist?

A. So a company that's using AWS compute service may create keypairs so the company itself can internally log-in to those virtual servers.

Q. Would the company have authorization or ask Capital One to do that?

A. Well, you're referring --

Q. Oh, sorry --

A. -- for ourselves -- and, yes, if they existed, it would be meant for internal use by the company.

Q. And does Capital One just generally authorize members of the public to create keypairs?

A. No, not all.

Q. Or if there are existing keypairs, to use those to access its computers?

A. No, not at all.

Q. Did the commands to describe keypairs, did those succeed?

A. No.

Q. I assume you tell us that based on the right-hand column?

A. Yes.

Q. Would the message in the right-hand column here also have gone to Ms. Thompson?

A. Yes.

Q. There are also, apart from the create keypair and describe keypair commands, there are four at the bottom, I believe. I'm not seeing them.

I'm sorry. The next four commands, if we can look at those. Those are also April 19th, so lines 39 to 42?

A. Yes.

Q. So those are four more events that took place on April 19th?

A. Yes.

Q. What command was issued for those four events?

A. "List-buckets."

Q. And did that command succeed?

A. I believe it did. If you scroll to the right, there would be no error message. Yeah.

Q. I'm sorry. I misdescribed the date for these. There are two dates that these actually took place, correct?

A. Can we scroll back to the left? I think these four are all on the 19th.

Q. Okay. And then let's go down because there will be two, I believe, on April 21st. Do you see two on April 21st?

A. Yes.

Q. Are those also list-bucket commands?

A. Yes.

Q. And were those successful?

A. Yes.

Q. Now, is April 21st a date that you've already seen in this case?

A. Yes.

Q. What is that date?

A. The gist that showed commands being executed, I believe, was the 21st.

Q. And so would one of these commands be the command that resulted in the creation of the April 21st gist?

A. Or vice versa, depending on -- yes, I believe they are linked.

Q. Why do you say "vice versa"?

A. Well, the commands that we see in the gist would have executed the events that were then placed in these logs.

Q. Okay. But they're associated?

A. They're one-for-one, yes.

Q. The same commands has resulted in both traces?

A. Yes.

Q. Fair enough.

And then if we just turn to the last line of the spreadsheet, what is the last date for an event that you see linked to Ms. Thompson?

A. May 26th.

Q. Is that the last date of activity, that Capital One is aware of, in connection with this breach?

A. Yes.

Q. In hindsight, has Capital One looked back and seen whether there were any warnings or alerts triggered during this breach?

A. Yes.

Q. And what did you find when you do that?

A. There were two cases opened and investigated by our operations center.

Q. When was the first case?

A. On the 22nd, I believe.

Q. Of March?

A. Of March, yes.

Q. The date of the exfiltrations?

A. Yes.

Q. And what caused that event or what triggered that?

A. It was an alert on failed get-object requests.

Q. Can you say what you mean by that?

A. So our monitoring and detection program looks at event logs, and for certain kinds of events will create a case for investigation, and one that we had a rule for and created a case for was multiple failed attempts to get -- to do a get-object command.

Q. And when you say "multiple failed attempts," how does that relate to what we've just talked about?

A. So in the spreadsheet with the four tabs, you know, one of which was a "failed to get-objects request," essentially, all of the log entries represented in that tab were related to a case that was opened.

Q. Okay. So the successful request did not trigger a case, but the failed ones did?

A. Correct.

Q. What happens when a case is triggered?

A. Someone in our operations center investigates it.

Q. And did someone do that in this case?

A. Yes.

Q. And what happened when they looked at and investigated?

A. They saw failed requests. They did not identify anything that, to them, looked like successful activity, and they closed the case.

Q. Okay. What was the second alert or warning in hindsight?

A. Later on, there was a second credential exfiltration alert.

Q. Okay. When did that happen?

A. I don't actually recall the precise date. I think it was in April.

Q. Was it in hindsight? Does it appear to have been triggered or linked by commands reflected in the CloudTrail log we just looked at?

A. Yes.

Q. And so when you say "credential exfiltration," what, specifically, was it?

A. So we use the AWS GuardDuty service, and credential exfiltration is the term that the GuardDuty service uses for this alert.

But, basically, it is looking for one of our credentials being used from outside of our environment, not from one of our resources. So it's an indicator that a credential has been stolen.

Q. In this case, is it the ISRM-WAF-Role being used in an external IP address?

A. Yes.

Q. And was an analyst assigned to that one?

A. Yes.

Q. And what did the analyst find?

A. They, again, failed to identify anything that looked like a successful data exfiltration or anything on that day and closed the case and moved on.

Q. Okay. Did they leave a note in the file about anything for the future?

A. Yeah. Basically, they said they didn't think that the traffic was necessarily, you know, something that we should -- it's called "whitelist," but, basically, not alert on, and to keep an eye out if it happened again.

Q. Are you aware of a handwritten note relating to -- that came up in the course of this investigation?

A. Yes.

Q. Okay. And would you take a look at Exhibit 952 and tell me if you recognize that?

A. Yes.

Q. Is that the note?

A. Yes.

Q. Did that note come to Capital One?

A. Yes.

Q. And when did that happen?

A. I believe it was in May.

Q. So how does that relate in time to when the data had been stolen from the company?

A. It was well after the date it had been stolen.

Q. A couple months?

A. Yes.

Q. Okay. There is an IP address in the middle of that. What is that IP address?

A. That is the same IP address we saw before, which was the WAF and web server that Ms. Thompson exploited.

Q. Okay. And there's a reference above that or there's a line above that that says "open SOCKS proxy"?

A. Yes.

Q. What is a SOCKS proxy?

A. A SOCKS proxy is a different kind of proxy, most commonly used to get out of a corporate network and get to the Internet. It has its own SOCKS protocol and port.

Q. Okay. Do you know what port number that is?

A. I believe it's 1080.

Q. Not 443?

A. No.

Q. Does this describe the misconfiguration that Ms. Thompson used to get access to Capital One data?

A. No.

Q. And why do you say that?

A. Because there was not a SOCKS proxy, much less an open SOCKS proxy.

Q. When you say "there was not a SOCKS proxy," does every port not have each proxy?

A. So a SOCKS proxy is a piece of software that you have to install and run, and there was no software that would act as a SOCKS proxy on the machine in question.

Q. Okay. So Capital One hadn't even installed the software this refers to?

A. Right.

Q. Was this note originally provided -- do you know the source of this note?

A. Capital One received it from AWS.

Q. Do you have any further knowledge beyond that?

A. No.

Q. And Capital One, I guess, investigated, you said?

A. Yes. In May, when this was received, a team -- like I said, the first step is to try to understand the veracity and can you reproduce the alleged vulnerability, and so the team attempted to and could not.

Q. And when the team was unable to produce or see this vulnerability, what did it do?

A. Closed the investigation.

Q. Are you aware of the volume of records or data that were taken during this breach?

A. Yes, in general terms.

Q. In general, how many people's data was taken?

A. It was about 98 million U.S. persons' data, and another six million Canadian persons' data.

Q. Did Capital One prepare an exhibit that summarizes the number of people's data?

A. Yes.

Q. Would you look at Exhibit 715 and tell me if you recognize that?

A. Yes.

Q. Is that the summary that Capital One prepared?

A. Yes.

MR. FRIEDMAN: The government offers 715.

THE COURT: 715 is a summary exhibit. Are you okay admitting it into evidence?

MR. HAMOUDI: I do have a little objection because it is a hearsay objection, but, also, I don't think -- I think there is another witness that can put this particular exhibit in.

THE COURT: Okay. I'll allow it to be displayed to the jury, but not admit it into evidence right now.

MR. HAMOUDI: Thank you, Your Honor.

Q. (By Mr. Friedman) Does this relate to all of the individuals whose information was taken, or just some?

A. All.

Q. Were there also Canadian citizens?

A. Yes. I'm sorry. This is the United States table. There is also a Canadian table with smaller numbers.

Q. But this is all U.S. citizens?

A. Yes.

Q. And how many U.S. citizens' data was taken?

A. Nearly 98 million in total.

Q. And was it the same data for each of those people?

A. No. There were a variety of different files that had different combinations of information, and so there is different tallies for different kinds of information for those individuals.

Q. And so it looks like, for most of the individuals, their name, their date of birth, and their self-reported income was taken?

A. Yes.

Q. What about addresses, say, mailing addresses?

A. Yeah. That was about 20 million of the individuals had mailing addresses, I think, exposed.

Q. How many people's Social Security numbers?

A. It was 117,000.

Q. What about bank accounts?

A. Almost 78,000.

Q. This was prepared a couple of years ago; is that correct?

A. Yes.

Q. Does Capital One still believe those are the correct numbers?

A. Yes.

Q. Mr. Fisk, are you aware that a search warrant was executed at Ms. Thompson's residence?

A. Yes.

Q. Did the government subsequently provide Capital One with data retrieved from Ms. Thompson's computer?

A. Yes.

Q. Have you looked at portions of that data?

A. Yes.

Q. I'm going to ask you to look at Exhibit 711. Tell me if you recognize that.

A. Yes.

Q. Is this a file structure or a list of files for that data that was provided to Capital One?

A. Yes.

MR. FRIEDMAN: Government offers Exhibit 711.

MR. HAMOUDI: No objection.

THE COURT: 711 is admitted into evidence.

(Government Exhibit 711 admitted.)

Q. (By Mr. Friedman) Mr. Fisk, do you recognize the files listed there, or buckets listed there?

A. Yes. All the things in the right-hand column are Capital One bucket names.

Q. Have you also looked at individual files or parts of individual files?

A. Yes.

Q. Would you take a look at Exhibit 712 and tell me if you recognize that?

A. Yes.

Q. In general terms, what is this?

A. Well, the lower right-hand corner, the one being highlighted, that is data from a file in a Capital One bucket that was stolen during this incident.

MR. FRIEDMAN: Government offers Exhibit 712.

MR. HAMOUDI: I object, Your Honor. I don't think he generated this data. I don't think he analyzed this data.

THE COURT: Well, do you want to ask any more questions about that?

MR. FRIEDMAN: Yes.

MR. HAMOUDI: That would be great, Your Honor.

Q. (By Mr. Friedman) Did you compare this data to data in Capital One's possession that you received from Capital One?

A. Yes.

MR. HAMOUDI: Objection withdrawn.

THE COURT: Thank you. I'll admit Exhibit 712 into evidence.

(Government Exhibit 712 admitted.)

Q. (By Mr. Friedman) Part of this screen is data, correct?

A. Yes, the lower-right quadrant.

Q. Do you have a general understanding of what the screen is overall?

A. Based on the title, it appears to be a forensics tool.

Q. And does it list a number of files or directories on the left-hand side?

A. Yes.

Q. Do you recognize those?

A. Yes. Those are Capital One buckets and directories.

Q. And then one that is highlighted, is it your understanding that the data shown in the bottom right comes from that file?

A. Yes.

Q. Did you compare it to that file retrieved from Capital One?

A. Yes.

Q. And what did you find?

A. We found these precise records on the screen in that file to verify the complete match.

Q. So what did you conclude based on that?

A. This was the same file that originated from us and was taken in the breach. We also saw the file name, specifically, in the event logs.

Q. And zooming in on the data, what type of data is this?

A. So this is, you know, data stored for use by computer programs but relating to credit card offers. You'll see statements, a sort of form-letter-looking formatting that says, "You are preapproved for this Capital One starter card offer," for example, and then contains the personal information of the customers or potential customers that that offer would be made to.

Q. And what personal information do you see for each customer? Do you see a name?

A. Yes. I see a first name; a middle name, or at least an initial; and last name.

Q. Do you see, towards the right, something that says, "addr line one"?

A. Yes.

Q. What is that? What type of information would that be?

A. That's the first line of a mailing address for the person's postal address.

Q. And we're just seeing gray here in the Capital One version?

A. Yeah, I've seen the actual address, yeah.

Q. And in the version the FBI provided you, was the actual address there?

A. Yes.

Q. So it's just been redacted for public display?

A. I presume.

Q. Do you also see, towards the left, date of birth as some of the information?

A. Yes.

Q. Did this file contain people's complete dates of birth?

A. Yes.

Q. And do you see "last four SSN" to the right?

A. Yes.

Q. What does "last four SSN" mean to you?

A. The last four digits of the person's Social Security number.

Q. And so this file contained that information?

A. Yes.

Q. If you would look at Exhibit 713. Is that also data provided to you by the government that you reviewed?

A. Yes.

Q. And did you compare that to Capital One data?

A. Yes.

MR. FRIEDMAN: Government offers Exhibit 713.

MR. HAMOUDI: No objection to this, Your Honor.

THE COURT: 713 is admitted into evidence.

(Government Exhibit 713 admitted.)

Q. (By Mr. Friedman) Now, this is in a file format that's hard to see, correct?

A. Yes.

Q. The exhibit has very long lines, correct?

A. Yes, it does.

Q. If we effectively scroll to the right to the fourth page of it, and let's zoom in on some of the data.

What type of information does this file contain?

A. You can see here it has address lines; again, it has last names; and I think, before we zoomed in, I could see first names as well.

Q. So it contained people's names and addresses?

A. Yes.

Q. And if we move one screen to the right, do you see there the types of information this file contained for the customers whose names were on the last screen?

A. Yes, date of birth and Social Security number.

Q. And did you compare this to the file that you got from Capital One?

A. Yes.

Q. And what did you find?

A. It matched exactly.

Q. Did you reach a conclusion based on that?

A. Yeah. It was our file that had been taken and then recovered by the FBI.

Q. Okay. And then I'm going to ask you to go back to Exhibit 712, which is the first piece of data that you compared. And if we could go to the second page of this exhibit.

Is this an additional portion of that file that you compared Capital One's data to the FBI's data?

A. Yes, this is additional data we compared.

Q. Okay. We'll zoom in on a few rows.

So what types of information in this case was in the data taken by Ms. Thompson from Capital One?

A. It has many of the same elements: date of birth, last four of Social Security number, full names, address, and then also some email addresses.

Q. Okay. And here, this is 712, it says "last four SSN"?

A. Yes.

Q. When we looked at 713, was that the four, or was that the full Social Security numbers?

A. I'd have to look again. We've seen examples of both, I think.

Q. Go back to 713, page 5, please.

A. Yeah, these were full numbers, I believe.

Q. Okay. Some of the 100,000 or so individuals whose full Social Security numbers were taken?

A. Correct.

Q. Thank you.

Mr. Fisk, is Capital One regulated by any government entity?

A. Yes, multiple.

Q. Is there a particular primary regulator?

A. Well, I think all of our regulators think they are primary, but the Office of the Comptroller of the Currency, in particular, regulates us.

Q. Is this a government entity that regulates banks or a portion of banks?

A. Yes.

Q. Do they show up every year to look at Capital One, or do they have people on-site permanently? How does that work?

A. They have what's called "resident examiners," people who, or at least pre-COVID times, would sit in the building but who we interact with regularly, and then they also schedule periodic exams.

Q. How regularly do they do the periodic examinations?

A. There're multiple annual cycles, so we see them more than once a year, but you can think of them as annual exams.

Q. As part of their examination, did they look at Capital One's cyber security following this breach?

A. Following the breach? Yes.

Q. And did they make any findings regarding Capital One's Cyber Security Organization and cyber security, I guess?

A. Yes, there was a consent order issued.

Q. Would you look at Exhibit 953? Do you recognize that?

A. Yes.

Q. What is that?

A. That is the consent order from the OCC.

Q. Okay. Did this reflect what the OCC classified as findings -- some findings they made?

A. Yes.

Q. Are those shown on the second page?

A. I believe so.

Q. If we could go to the second page. There is a section, Article II, it says, "The Comptroller finds, and the bank neither admits or denies," do you see three findings after that?

A. Yes.

Q. What did the comptroller find?

A. To summarize concerns with the risk-management process around information technology and NAC operations, is what the first one describes.

Q. So the first one, would you just read the first sentence of the first one?

A. "In or around 2015, the Bank failed to establish effective risk assessment processes prior to migrating its information technology operations to the cloud operating environment."

Q. What was the second finding?

A. That our internal audit team at the bank had not identified some of the gaps and weaknesses.

Q. And what was the third finding?

A. That the Board had not driven sufficient action around issues.

Q. Were these findings general findings, or did they relate to specific events?

A. They're fairly broad and reflect, I believe, the OCC's perspective over examining us over an extended period.

Q. Did this whole consent order include a financial penalty for Capital One?

A. Yes, it did.

Q. And how much was that penalty?

A. $80 million.

Q. Was there also a separate consent order that talked about procedures and going forward?

A. Yes.

Q. And in general terms, without going to it specifically, do you understand, generally, what that provided?

A. There were a bunch of enhancements to our security program at the bank that we planned to make and that they would supervise the execution of.

Q. Do either of those orders refer specifically to this breach or the events of this breach?

A. No.

Q. Were they all more general and procedural?

A. Yes, and much broader.

Q. Did either of them refer to Ms. Thompson?

A. No.

Q. Did either of them make any findings about whether Capital One had authorized or permitted Ms. Thompson to do anything?

A. No.

Q. Was there any reference at all to this breach in those orders?

A. No, not to my knowledge.

Q. Has Capital One one also conducted its own evaluation of what happened?

A. Yes.

Q. And did you participate in that evaluation?

A. Yeah. Actually, very early on, I was asked to lead that investigation.

Q. And what did you find, in general terms?

A. You know, the most -- the primary things we identified were the things we've discussed around the misconfiguration of the WAF, the fact that WAF role had, additionally, been given overly broad access to data that it didn't need under principle of least privilege.

Q. Those all sound like technical findings about what happened.

A. Yes.

Q. Were there also broader findings about Capital One as an entity?

A. Yes. There were some procedural things; for example, much of the reason that Social Security numbers were in the data that was stolen. Well, the examples we saw here, I think, looked like individuals. In many cases, they were associated with small-business cards, and a small-business owner has a tax ID number that may be a company tax ID number, but personal proprietorship may be an individual's Social Security number used as a tax ID number. And so, for example, there were some gaps in our software developers understanding that a small-business tax ID number needed to be protected the same that we protect a Social Security number in our standards, for example.

Q. Okay. Were there also findings about Capital One's overall Cyber Organization structure and company structure, things like that?

A. Yeah. There were some statements around, sort of, ambiguities in people's roles.

Q. Did Capital One -- I think you've described this breach as resulting from a misconfiguration and other configurations and things like that. Is it fair to say "a mistake" or "mistakes"?

A. Yes.

Q. Did Capital One ever intend for the data that Ms. Thompson took to be available to the public?

A. No, never.

Q. Does Capital One intend for its banking data to be available to the public, ever?

A. No.

Q. Would it be legal for Capital One to make that data just generally, publically available?

A. No. The Gramm-Leach-Bliley Act, amongst others, I think protects consumers and says their information needs to be kept private.

Q. Did Capital One intend for Ms. Thompson to be able to assume the role that she assumed?

A. No.

Q. Did it intend for Ms. Thompson to be able to access any data?

A. Not unless she was a customer and accessing only her specific -- data of her own, but not the data she accessed.

Q. Did Capital One ever do anything that you view as authorizing or allowing her to do that?

A. No.

Q. So how did you explain what happened here?

A. Capital One, we had made some errors and mistakes in configuring things, and that made it -- created a vulnerability that she was able to find and exploit.

MR. FRIEDMAN: Thank you very much.

THE COURT: Okay. We'll take our mid-morning break now, and then come back with cross-examination of Mr. Fisk.

So leave your notepads and pens on your chairs, and please stay in your seats in the audience until the jury has an opportunity to be taken downstairs by the courtroom deputy.

(Court in recess 10:30 a.m. to 10:50 a.m.)

THE FOLLOWING PROCEEDINGS WERE HELD
IN THE PRESENCE OF THE JURY:

THE COURT: We will now do cross-examination of Mr. Fisk by Mr. Hamoudi.

MR. HAMOUDI: Good afternoon, Mr. Fisk.

THE COURT: Or good morning.

MR. HAMOUDI: Good morning, Mr. Fisk.

THE WITNESS: Good day.

CROSS-EXAMINATION

BY MR. HAMOUDI:

Q. Capital One has represented that this incident involved the granting of overly permissive access to its web access firewall roles; correct?

A. I think it -- I think you're mixing two statements. Overly permissive permissions with respect to the S3 buckets was a factor; and then secondly, a misconfiguration of the WAF.

Q. Okay. And when you say misconfiguration of the WAF, you mean configuration; correct?

A. Yes.

Q. Okay. And so the incident really involved a gap in access management by Capital One; correct?

A. I believe that was a secondary factor, with the WAF configuration being the primary.

Q. Ms. Thompson was able to access your AWS storage from outside the Capital One network because of a lapse in access management; correct?

A. Primarily because she stole the credential.

Q. Okay. Did you previously testify in a proceeding under oath?

A. I've been deposed under oath, I guess.

Q. Okay. And do you remember being asked whether Ms. Thompson received access to the Instance Metadata Service? Do you recall being asked that question?

A. Uhm, it's been a while, so, no, not precisely, but...

Q. Okay. Do you remember saying that she didn't take the credentials, I wouldn't say that, she got access to the metadata service which provides the credential?

A. I may have said that, sure.

Q. Okay. Would it help refresh your recollection if I show you the portion of your testimony that you gave under oath?

A. Yes.

Q. Okay.

MR. HAMOUDI: Can you bring up CONE1903, please?

THE COURT: This is just going to be shown to the witness, not to the jury.

Q. (By Mr. Hamoudi) And this is your deposition.

MR. HAMOUDI: Can you go down to page 88, CONE1903. And up there at the top.

Q. (By Mr. Hamoudi) And you were asked a question, Once she was able to get into the metadata service, she took the credential and that allowed her to gain access to the card prod account and the 7 to 800 S3 buckets.

And what is your answer to that?

A. So I was saying that she utilized the metadata service, not that she broke into the metadata service.

Q. Can you -- but can you answer what you said under oath?

THE COURT: Just read the answer.

A. Just read the answer?

Q. (By Mr. Hamoudi) Yes.

A. I wouldn't say that -- sorry, I wouldn't say that she got into the metadata service, she essentially got access to the metadata service, which provides the credentials, which, as you said, then provided access to the -- to data.

Q. Okay. Thank you.

Now, I want to go back and ask you, Capital One configured the web access firewall -- you can take that off the screen -- Capital One configured the web access firewall to allow external computers to retrieve credentials from Capital One's Instance Metadata Service, didn't it?

A. That may have been the effect, but an employee of Capital One enabled proxying on the WAF, and Ms. Thompson discovered that that would allow her access to the Instance Metadata Service, but that was never an intent of the company.

Q. So Capital One configured the web access firewall?
A. Yes.
Q. Okay. And Capital One could have configured the web access firewall to deny external requests; correct?
A. Yes.
Q. And Capital One could have configured the web access firewall to deny external requests from iPredator?
A. Yes.
Q. From TOR?
A. That would be difficult since TOR uses IP addresses all over the Internet.
Q. But it could have?
A. At the risk of disenfranchising our customers and potentially breaking the law in terms of not allowing them to have access.
Q. So you agree that some of your customers may use TOR to access your services?
A. I guess they might.
Q. Okay. And the permissions on AWS servers are set by the user, Capital One; correct?
A. Yes.
Q. And AWS servers are zero permission by default; correct?
A. Essentially.
Q. And so Ms. Thompson only had permission to access Capital One's web access firewall because Capital One granted her such

permissions; isn't that correct?

A. So the web application firewall was configured by Capital One to be Internet facing, because that was its purpose, to serve customers on the Internet.

Q. So I'm going to ask the question again, and say "yes" or "no." So Ms. Thompson only had permission to access Capital One's web access firewall because Capital One granted her such permissions?

A. Yes.

MR. HAMOUDI: Okay. If we could go to Exhibit 205, please, which has been previously admitted.

Down at the bottom, if you could blow it up, it says HTP200, okay?

Q. (By Mr. Hamoudi) You provided some testimony on this part of the April 19, '21 gist log. Do you recall that?

A. I think it was April 21st of 2019, but, yes.

Q. My apologies, April 21st, 2019.

Wasn't Capital One's servers responsible -- wasn't Capital One's server's response to Ms. Thompson's CURL command here "okay"?

A. I think this response actually came from the instance -- AWS Instance Metadata Service.

Q. And Capital One configures the Instance Metadata Service; correct?

A. The Instance Metadata Service is not very configurable by the AWS customer.

Q. So I'm going to ask the question again. "Yes" or "no," wasn't Capital One's server's response to Ms. Thompson's curl command "okay"?

A. She received an "okay" response, yes.

Q. Okay. And that's from the server; correct?

A. AWS Instance Metadata Service.

Q. And it could have responded forbidden or unauthorized?

A. Yes.

Q. And if Ms. Thompson set her --

MR. HAMOUDI: Let's go back to the top where -- http 169, yes, if you could zoom that up.

Q. (By Mr. Hamoudi) and you gave some testimony about the http -- and what is http?

A. It's the Hypertext Transfer Protocol. We think of it as the protocol for the web.

Q. And it doesn't have an S after the P; correct?

A. Correct.

Q. And that distinction is important; correct?

A. It can be.

Q. And why is that distinction important?

A. So http without the S implies that the traffic is not encrypted.

Q. Okay. So if Ms. Thompson set her web browser to use Capital One's web access firewall as a proxy, couldn't she have just typed the http language, the URL, into her browser and gotten the same credentials?

A. Yes.

Q. Okay. And Port 443 is also a public port; correct?

A. I don't know if the ports are inherently public or not, but, yes, this firewall made 443 available to the Internet.

Q. Well, it's for traffic -- for public traffic; correct?

A. I mean, companies use 443 for internal private traffic as well, but, yes this was an Internet-facing server.

Q. So I want to talk about the CloudTrail logs and the GuardDuty responses, the signals that you testified on direct. Do you recall that testimony?

A. Yes.

Q. Okay. So on direct, you testified --

MR. HAMOUDI: You can take that down. Thank you so much.

Q. (By Mr. Hamoudi) So on direct, you testified that Capital One reviewed the CloudTrail and GuardDuty logs in March 2019; correct?

A. I said there were GuardDuty -- there was a GuardDuty alert that was reviewed in March of 2019. The CloudTrail logs we collected, the forensic analysis was done in July after discovery of the breach.

Q. So the GuardDuty logs were reviewed in March 2019?

A. The GuardDuty -- the GuardDuty logs are collected and an automated system creates cases for investigation based on some of them. And we discussed one case from a GuardDuty alert that was created on March 22nd.

Q. And these were Capital One analysts; right?

A. Yes.

Q. And trained cyber security professionals?

A. Yes.

Q. And they saw that an external user was accessing Capital One's web access firewall; right?

A. I don't recall if they noted that it was external or not on that one.

Q. It was coming from iPredator; correct?

A. It was. I do not recall if that was noted in the case or not.

Q. And they didn't block the user, did they?

A. The -- blocking the ISRM-WAF user would have taken down services.

Q. But you could have blocked the individual user if you wanted to, as a trained cyber security professional; correct?

A. So Ms. Thompson was acting with the stolen identify of the WAF, so blocking Ms. Thompson, and by identity, would have blocked the legitimate WAF as well.

Q. So the system was treating her as a legitimate user?

A. Yes, because she was impersonating one.

Q. Okay. Well, you talk about impersonating. You haven't met my client; correct?

A. Not -- not closer than today.

Q. Okay. And you've never sat down and had a conversation with her, have you?

A. Correct.

Q. So when I ask questions about the system, if you could focus on what technologically happened, I would greatly appreciate it.

I want to follow up, you used the term on direct "whitelisted." What does whitelisted mean?

A. It is enumerating a set of things to allow, or in that context to not alert on.

Q. What about blacklisted?

A. It is a term to enumerate a set of things to not allow.

Q. Okay. And despite Capital One's review of its GuardDuty logs from March 2019, Capital One's analyst did not blacklist the IP address, which is attributed to my client, to it, did it?

A. Correct.

Q. Okay. I want to talk about data a little bit.

MR. HAMOUDI: Have Exhibit 715, please.

Q. (By Mr. Hamoudi) How old was this data?

A. Much of it went back, you know, a number -- several years. I don't recall the precise direction, but it's collected over a long period of time.

Q. And Capital One didn't encrypt the data; right?

A. It was all encrypted as it was stored. And additionally, a lot of the information is further tokenized or encrypted. But what was taken was taken in decrypted form.

Q. So the data that was taken, before it was taken, it was not encrypted; correct?

A. No. It was encrypted and stored encrypted in S3.

Q. Okay. But the data, the content, the substance of the data was not encrypted; correct?

A. No, it was encrypted.

Q. Which data was encrypted?

A. All of it.

Q. Okay. Are you dis- -- is there a distinction between tokenized and encrypted?

A. Yes.

Q. Okay. You're not aware that Ms. Thompson ever used or shared Capital One's data with anybody; correct?

A. I'm not aware of that, that she did, no.

Q. Okay. And if Capital One learned of that, they would have immediately informed regulators; correct?

A. Correct.

Q. And she didn't have to decrypt the data as she took it; correct?

A. S3 decrypted it for her because she had the credential.

Q. Okay. And you're not -- strike that.

I want to go back and talk about the data, since we're on that.

No credit card account numbers or login credentials were compromised; correct?

A. Correct.

Q. And over 99 percent of the Social Security numbers were not compromised; correct?

A. Correct.

Q. And the largest category of information was routinely collected information; correct?

A. I'm not sure what you're referring to by "routinely collected."

Q. Routinely collected in the course of business, name, address, phone number, date of birth; correct?

A. Yeah. I mean, I would say all of this information was collected in the course of business.

Q. Okay. And then when we talk about data, the total number of data was -- it was upwards of 1.7 terabyte; correct?

A. Yes, something -- it was large, yeah.

Q. Okay. So when we're talking about data, the 1.7 terabyte, how much of that data was the data that is represented on Exhibit 715?

A. In terms of storage space, it was probably a relatively small fraction. Some of the individuals -- you know, an individual's name, for example, may have occurred multiple times in multiple files, so this is a unique count per person.

Q. Okay. And in terms of understanding how long it would take to go through 1.7 terabytes of data, can you give us a sense of how long it would take for someone to go through 1.7 terabytes of data given your experience with data?

A. I mean, if I wanted to, you know, look for Social Security number, for example, I can, you know, issue a command that searches for the right sort of pattern. And it would probably take at least hours, depends a little bit on if you're just doing it on your laptop or if you're -- you know, have a big server in the cloud or how you're doing it.

Q. Okay. I want to talk about the web access firewall.

Who was the -- who was the -- who's Houston Hopkins?

A. Houston Hopkins was a member of the security team at Capital One.

Q. Did -- was he supervised by you?

A. No.

Q. Did he report to you?

A. No.

Q. And were you colleagues?

A. We were both members of the same organization.

Q. Okay.

A. Worked with him.

MR. HAMOUDI: May I approach, Your Honor?

THE COURT: Sure.

THE CLERK: Do you want me to mark this, Counsel?

MR. HAMOUDI: I'm not going to admit it, I'm just going to talk to him, unless the Court would like me to.

THE COURT: I think we should put an exhibit number on it, yeah.

MR. HAMOUDI: Okay. What's next?

(Off the record.)

MR. HAMOUDI: 1202.

THE COURT: Okay. Exhibit 1202 is marked for identification.

Q. (By Mr. Hamoudi) Take a moment to review that. And let me know when you're finished.

A. Okay.

Q. Okay. And help me understand, what is the platform, this messaging, that you and Mr. Hopkins are having together?

A. I suspected it was from Slack, which is a chat system that we use.

Q. And what is Slack?

A. It's a commercially available chat service that companies use.

Q. And you're having this discussion internally between you and Mr. Hopkins?

A. Yes.

Q. And this is a private conversation; correct?

A. Yes.

Q. Okay. And in this conversation, he, as your colleague, security colleague, takes the position that we should stay away from the term "misconfiguration," which looks like we have mostly done; is that correct?

A. He says that, yes.

Q. And he also says that the web -- the mod_proxy set to the Proxy Requests on was also purposeful; correct?

A. He states that as his opinion.

Q. That's his opinion; correct?

A. Yeah.

Q. And he memorializes that opinion in this private Slack chat channel with yourself; correct?

A. I'm not sure if there's a legal meaning to memorialize, but he said it.

THE COURT: It's not a proper question.

MR. HAMOUDI: I apologize. I strike that, Your Honor.

THE COURT: Sure.

Q. (By Mr. Hamoudi) But he put it -- he was sending his thoughts to you; correct?

A. Yeah, in a conversation with me, he said this.

Q. Yeah.

And you disagree with that opinion, you had a -- you differ. You didn't believe that that was purposeful; correct?

A. I disagreed the configuring that way was the right configuration.

Q. Okay. Was the right configuration.

A. Yeah.

Q. So -- and as two security professionals, you just had a disagreement of opinion; correct?

A. Essentially.

MR. HAMOUDI: Okay. All right. I want to mark for identification 12 -- 1012.

THE CLERK: That was already marked, Counsel. Can we use --

THE COURT: Just the next number you want?

(Off the record.)

MR. HAMOUDI: Oh, that one was 1015?

THE COURT: No, this is 12 --

MR. HAMOUDI: 1015.

THE COURT: Okay.

(Off the record.)

MR. HAMOUDI: I apologize, Your Honor. We premarked this as 1012. I think I just used -- jumped.

THE COURT: So you want to show it to Victoria and see if it is 1012 in her book or if it needs a new number?

MR. HAMOUDI: Yes.

THE CLERK: We had already marked Ms. Valentine's LinkedIn profile as 1012, so can I just change it to 1013?

MR. HAMOUDI: Yes. I apologize.

THE COURT: That's marked as 1013 now.

MR. HAMOUDI: Oh, can I have a copy back, please?

THE COURT: Yeah.

Q. (By Mr. Hamoudi) Mr. Fisk, let me know when you finish reviewing 1013.

A. Okay.

Q. This is an email that was sent from an individual named Robert McLean; correct?

A. Yes.

Q. And Robert McLean, who is he?

A. He works in the Capital One cyber security organization on threat intelligence.

Q. Do you supervise him or are you colleagues?

A. I do not supervise him, but we're both in the same organization.

Q. Okay. And this email was sent at or near the time the incident happened?

A. It was sent on August 2nd of 2019.

Q. Yeah.

And this email is kept in the course of Capital One's regularly conducted business activities?

A. I'm not sure. Can you restate the question, or I'm not sure what you mean.

Q. Yeah.

Do you regularly send emails as part of your business practice internally within Capital One to --

A. Yes.

Q. -- your fellow colleagues?

A. Yes.

Q. And this email represents that?

A. Yes.

MR. HAMOUDI: Okay. And at this time, Your Honor, I'd like to move to admit Exhibit 1013 under the business records exception.

MR. FRIEDMAN: Objection. I don't think it qualifies.

MR. HAMOUDI: The alternative, non-hearsay purposes, Your Honor, that Capital One was on notice as to the substance of this email. And I will link it back through the Special Agent Martini when he testifies about whether or not he was given this information when he initially started the investigation.

THE COURT: Well, I'm not going to admit the exhibit into evidence, but, again, if you want to ask Mr. Fisk questions about its content, that's fine.

MR. HAMOUDI: Okay.

Q. (By Mr. Hamoudi) So let me ask you this, this is an email from Mr. McLean to yourself; correct?

A. I'm copied on it, yeah.

Q. Yes.

And in this email, Mr. McLean is expressing a, we are confident in that individual, Lila Ghosh's discovery; correct?

A. Yes.

Q. And here they're talking about the note that was previously admitted; correct?

A. They don't state it, but I believe that is probably the case.

Q. That's the case.

And the assessment of the cyber security team at Capital One was that either Ms. Thompson or her associate Neoice was the source of that note; correct?

MR. FRIEDMAN: Objection. He's effectively reading the contents of the note.

THE COURT: I'll allow the question.

You can answer.

A. Sorry, could you restate the question?

Q. (By Mr. Hamoudi) Yeah. And the assessment here is that either Ms. Thompson or her associate Neoice was the source of that note; correct?

A. It was our threat intel team and Bob's team's assessment. Yeah, they had confidence in their theory that the note may have been passed at a Sheraton down the street from the conference.

Q. All right. Thank you.

Just continue on there.

Marked next in order, Defendant's Exhibit 1014.

A. Okay.

Q. Have you seen this email before?

A. Not that I recall.

Q. Not that you recall.

Were you aware that Capital One employees believed that Ms. Thompson's activity on May 26th accessing Capital One's servers was presumably to check to see if the credential system would grant access after passing the note. Were you aware that Capital One employees believed that?

A. We certainly believed that the attempt was to see if the access still existed. I wasn't aware of this -- yeah, this theory that it was specifically after passing a note.

Q. Okay. Were you also -- were you aware that Capital One employees believed that the April 19th access that you discussed on direct examination was a confession scan or a loud and proud scan?

A. I did not.

Q. You did not?

A. I had not seen or heard that phrase before, no.

Q. And what is a confession scan?

A. It's not a term I've heard before, so I could speculate on what it means, but I --

THE COURT: You don't need to speculate.

Q. (By Mr. Hamoudi) Okay. Isn't it true that Capital One configured the role so that the role had permission to access the sensitive data that was downloaded by Ms. Thompson; correct?

A. Correct.

Q. And isn't it true that Ms. Thompson's actions caused

Capital One to change this configuration so that it was no longer available or -- to anyone; correct?

A. Our discovery of the actions, yeah.

Q. Okay. And so between March 12th, when I believe the first access was -- you testified to on a log, until July, other than Ms. -- other -- was there anybody else that let Capital One know that its servers were accessible?

A. No. The only notice we received was that note.

Q. Okay.

A. Sorry, the responsible -- the email note from Kat Valentine I'm referring to.

Q. Ms. Thompson could not see the data before she downloaded it; right?

A. She could see file names, she could not see what was in the file.

Q. And Ms. Thompson did not -- okay, that's fine. Let me move to the next.

The gist file, do you remember looking at the gist file?

A. Yes.

Q. You mentioned personally reviewing the gist Ms. Thompson posted onto GitHub; correct?

A. Yes.

Q. And it was easy for Capital One to reproduce the vulnerability with the information Ms. Thompson provided on GitHub; right?

A. Yes.

Q. And indeed, in your experience, isn't it true that sometimes people make information about vulnerabilities public to get them fixed; correct?

A. Yes.

MR. HAMOUDI: Can you bring Exhibit 207 up, please? Is this the special file? Oh, it is.

MS. MANCA: Victoria, would you mind turning off the...

(Off the record.)

MR. HAMOUDI: If you could go to the right where it says you are not authorized, Agent.

Yeah.

Q. (By Mr. Hamoudi) On direct, you testified that at times Ms. Thompson received a, you're not authorized response from Capital One servers. Do you recall that?

A. I said that AWS provides this error message intended to be delivered to the user initiating the request.

Q. But when you say "servers," these are servers that Capital One is leasing; correct? From AWS?

A. No. I would not describe it that way. The public APIs, interfaces that Amazon has, are on servers that we don't, you know, lease or contract for specifically.

Q. Okay. So at the times that there was no error, the servers did authorize Ms. Thompson's access; correct?

A. No. They responded to the requester who had stolen and was using a Capital One credential.

Q. Okay. If a certain computer allows a user to run commands on it, isn't it a reasonable conclusion for that person to believe they're authorized to do so?

A. No.

Q. Okay. You also testified that Capital One would have been interested in learning about external access to its security credentials; right?

A. Yes.

Q. The public wouldn't have known that in 2019; correct?

A. Sorry, could you restate the question?

Q. Yeah.

The public wouldn't have known that in 2019; correct?

A. Wouldn't have known what? Sorry.

Q. You testified that Capital One would have been interested in learning about external access to its security credentials; right?

A. Yes.

Q. The public would not have known that in 2000 --

A. Would not have known that there was public access, or that we would have been interested, or I'm not sure what you're asking.

Q. Yeah. The latter.

A. Would the public have known that we would be interested?

I --

Q. No, that it was accessible --

A. Would the public have known that there was -- that there was a vulnerability where someone could get the credentials, is that what you're asking?

Q. Yes.

A. Sorry. Don't mean to be obtuse.

Q. You're not being obtuse. I think I'm just not asking a very clear question.

A. I will grant that.

Q. I will take responsibility for that.

All right. You discussed the keypair on direct. Do you remember that?

A. Yes.

Q. Okay. The keypair does nothing without permission from the server; right?

A. Creating a keypair is creating a permission.

Q. But the server does that; correct?

A. The server will execute a keypair creation request if an authorized user presents a credential that allows them to do so.

Q. I guess the computer doesn't make a distinction between authorized and unauthorized, it doesn't assess motive; correct?

A. Correct; it just assesses, do you have the credential --

Q. And then if you have them, it will give them to you?

A. If you have a credential that has permission to create a keypair, it will create the keypair.

Q. And I want to make sure this is clear because the permissions are configured by -- is configured by Capital One; correct?

A. The permission of whether or not the role is able to create a keypair is configured by Capital One.

Q. Okay.

A. And it was denied because we had not granted that permission.

Q. But you did -- permission was granted on March 22nd when the data was downloaded; correct?

A. The permission to read data had been granted to the ISRM-WAF-Role.

Q. You talked about the OCC, which is short for the Office of the Controller of Currency; correct?

A. Yes.

MR. HAMOUDI: All right. Mark Exhibit 1009. Offer 1009.

MR. FRIEDMAN: No objection.

THE COURT: 1009 is admitted into evidence.

(Defense Exhibit 1009 admitted.)

MR. HAMOUDI: Publish 1009, please.

(Off the record.)

Q. (By Mr. Hamoudi) As part of Capital One's business activities, they issue annual reports to the public; correct?

A. Correct.

Q. And in 2020, do you recognize this document, this is an annual report issued by Capital One?

A. Yes.

Q. Okay. I want to turn your attention to a term on the next page up top. And in that report, it describes a cyber security incident; correct?

A. Yes.

Q. And what does it say?

A. It says Cyber Security Incident: The unauthorized access by an outside individual who obtained certain types of personal information relating to people who had applied for our credit card products and to our credit card customers that we announced on July 29th, 2019.

Q. Okay. And then if you go to the next page, and in the yellow, if you can read that out loud, the two paragraphs?

A. Yes. Sorry. Governmental Inquiries, sort of a heading font. We have received inquiries and requests for information relating to the cyber security incident from Congress, federal regulators, relevant Canadian regulators, the Department of Justice, and the offices of approximately 14 state Attorneys General. We are cooperating with these offices and responding to their inquiries.

The second paragraph says, In August 2020, we entered into consent orders with the Federal Reserve and the OCC resulting from regulatory reviews of the cyber security incident and relating to ongoing enhancements of our cyber security and operational risk management processes. We paid an $80 million penalty to the U.S. Treasury as part of the OCC agreement. The Federal Reserve agreement did not contain a monetary penalty.

MR. HAMOUDI: Okay. And then mark next Exhibit 1008. Offer 1008.

MR. FRIEDMAN: Your Honor, I think we've already offered that same document this morning.

THE COURT: I don't know that you actually offered it. You used it, but you didn't, so...

MR. FRIEDMAN: We certainly have no objection.

THE COURT: It's the content; right?

MR. HAMOUDI: Yes, yes.

THE COURT: 1008 will be admitted into evidence, sure.

(Defense Exhibit 1008 admitted.)

Q. (By Mr. Hamoudi) And if you go to the second page, the annual report referenced a consent decree. Do you recall the $80 million penalty?

THE COURT: Yeah. We just heard that.

MR. HAMOUDI: Oh, yes. Okay.

Q. (By Mr. Hamoudi) And go -- just reread the first paragraph, please, Article II, number 1.

A. Right. Under the part where it says, The bank neither admits or denies the following?

Q. Yes.

A. One, in or around 2015, the bank failed to establish effective risk assessment processes prior to migrating its information technology operations to the cloud environment. The bank also failed to establish appropriate risk management for the cloud operating environment, including appropriate design and implementation of certain network security controls, adequate data loss prevention controls, and effective dispositioning of alerts.

Q. And if you could go down to the second one as well?

A. Two, the bank's internal audit failed to identify numerous control weaknesses and gaps in the cloud operating environment. Internal audit also did not effectively report on and highlight identified weaknesses and gaps to the audit committee.

Q. And then the last one?

A. Three, for certain concerns raised by internal audit, the board failed to take effective actions to hold management accountable, particularly in addressing concerns regarding certain internal control gaps and weaknesses.

Q. And then if you go to the second page, please?

THE COURT: Third page.

Q. (By Mr. Hamoudi) The third page, please, and then Article III, section 1

A. Read it?

Q. Yes, please.

A. The bank shall make payment of a civil money penalty in the total amount of $80 million, which shall be paid upon the execution of this order.

Q. Okay. And so fair to say that one of the interests in a bank is to reduce its exposure to penalties by regulators that are imposed, such as this penalty?

A. Yes.

MR. HAMOUDI: Okay. No further questions.

THE COURT: Okay. Any redirect, Mr. Friedman?

MR. FRIEDMAN: Briefly, Your Honor.

MR. HAMOUDI: Your Honor, I made a mistake, apparently my colleague had some questions for me to ask and I did not ask them.

THE COURT: Well, I'll let you do it after Mr. Friedman.

MR. HAMOUDI: Okay. Thank you, Your Honor.

THE COURT: Sure. That way you can get straight what Mr. Klein is trying to get you to say.

MR. HAMOUDI: I apologize.

THE COURT: Okay. No problem.

REDIRECT EXAMINATION

BY MR. FRIEDMAN:

Q. Good morning again, Mr. Fisk.

A. Good morning.

Q. You were asked some questions about the data that was

downloaded in this case?
A. Yes.
Q. And the volume of that data?
A. Yeah.
Q. And I think you used the phrase "a lot of data"?
A. Probably.
Q. Are you aware of how long it took for that download to take place?
A. I believe it was the better part of a day, many hours.
Q. You were asked about a -- I think you were shown a document marked as Exhibit 1013, which would be in front of you. It was about what some Capital One employees might have believed?
A. Yes, regarding the conference?
Q. Yeah.
As an initial matter, was this a unanimous opinion at Capital One?
A. I would describe it as a working theory.
Q. Okay. Are there a lot of employees at Capital One?
A. There are.
Q. Do they -- some of them have different opinions about some things?
A. Of course.
Q. Okay. And does this email show some of the information on which this particular person's opinion was based?
A. Yes.

Q. Okay. Is it based on the assumption that this note was passed at a conference in Bellevue, Washington?

A. Yes.

Q. Is it based on the assumption that it was passed between April 29th of May -- April 29th and May 2nd of 2019?

A. Or thereabouts. It says those are the dates of the summit and --

Q. Okay. But those are --

A. -- summit, so...

Q. Fair to say those are --

THE COURT REPORTER: I'm sorry, one at a time.

THE COURT: One at a time.

MR. FRIEDMAN: Sorry.

Q. (By Mr. Friedman) Is it fair to say that those are assumptions that lead to whatever this person believed or concluded?

A. Yeah. I mean, it's stating the fact that a conference happened and the hypothesis that the note was passed and relating to a Sheraton hotel down the street.

Q. Okay. And is that a factor in whatever conclusions this person draws about who may have passed that note?

A. I mean, it's a fact that there's a Sheraton down the street, but that the note that we discussed earlier was passed, you know, near that Sheraton or at the time of this event is what I would describe as a working theory.

Q. Okay. But my question is, are those facts factors in this person reaching that opinion, is that part --

THE COURT: You know, we're asking a lot of questions that really are not pertinent here. So let's move on, Mr. Friedman.

Q. (By Mr. Friedman) You were asked questions -- I think a question, that is the reason -- to the effect of, is the reason that Ms. Thompson was able to download this because Capital One had given her permission to do that. Do you recall that?

A. Roughly.

Q. Okay. Do you recall saying that she was able to do what she had done because she had been given permission to do that by Capital One?

A. No.

Q. Okay. Would that be -- any time someone was able to breach a company using credentials, would that be because that person had used those credentials?

MR. HAMOUDI: I'm going to object to that, Your Honor.

THE COURT: Yeah. I think we're getting out into the ionosphere. The jury understands what's going on and the difference between getting somewhere and having permission to get somewhere, so let's move on.

MR. FRIEDMAN: Okay.

Q. (By Mr. Friedman) Did Capital One intend for Ms. Thompson to be able to assume the role that she assumed?

A. No.

MR. HAMOUDI: That's an ultimate issue, Your Honor. I'm going to object.

THE COURT: I'm going to overrule the objection.

You can -- the answer to that question was?

A. Was no.

THE COURT: All right.

Q. (By Mr. Friedman) And did Capital One intend for Ms. Thompson to be able to take that data?

A. No.

Q. If Capital One intended for that data to be publicly available, how might it have gone about making that data publicly available?

A. I mean, it's sort of a contrived question, given the nature of the data, but we have an open API system with documentation, so where we want to provide some, you know, technical access to a service, it's done through that, or for individual users, it's done through a web application or an app on your phone that you get an account for, and you log in using your credentials and get the access that we give you using your credentials.

Q. But it wouldn't require assuming a role from the Instance Metadata Service?

A. Right. It would not require using the WAF-Role.

Q. Okay. Did the method by which Ms. Thompson obtained that data, did it make that data available to anyone who didn't have a high degree of technical computer sophistication?

A. It took a lot of sophistication to identify that vulnerability and exploit it. It was not a well-known vulnerability.

Q. Okay. Are you aware of any conversations about -- at Capital One about making this data publicly available only to people with a high degree of technical ability?

A. No.

MR. FRIEDMAN: Okay. Thank you. I have no further questions.

THE COURT: All right. Mr. Hamoudi, you can ask the other questions and any other follow-up from what Mr. Friedman did.

MR. HAMOUDI: Can I have a moment, Your Honor?

THE COURT: Yeah, sure.

MR. HAMOUDI: Thank you.

RECROSS-EXAMINATION

BY MR. HAMOUDI:

Q. There was some discussion about that email. I just want to be clear, the email, which is Exhibit 1013, about the assessment about the note, it says in there, "we are confident," the assessment says that "we are confident"; correct?

A. Yes.

Q. And "we" is not just an individual, there's a collective "we"; correct?

A. So the sentence before that says, I enlisted the team. I believe "we" is referring to the team. And that is Robert's threat --

Q. Okay.

A. -- team.

Q. So Michael Johnson, who is he?

A. He was the chief information security officer at the time.

Q. Who is Jill Vaughan?

A. She was a deputy chief information security officer for governance and risk.

Q. Devon Rollins?

A. Bob McLean reported to him. He led our threat intelligence function.

Q. And who is Nicole Washburn?

A. She was also a manager in our operations and intelligence organization.

Q. And Mr. Friedman just asked you questions about data availability, public availability. Capital One did make the data publicly available, did it not?

A. No.

Q. Well, it was accessed through an http, correct, and it wasn't secure?

A. No, that's not correct.

Q. Well, I think we covered this in the exhibits.

MR. HAMOUDI: Can you bring up the gist file?

(Off the record.)

MR. HAMOUDI: 204, please. Or 205.

Go up top, please.

Q. (By Mr. Hamoudi) Right there it says http. Do you remember your testimony about that?

A. Yes.

Q. So any user who set their web browser up as a proxy could have punched that into their web browser and executed this command; correct?

A. Yes.

MR. HAMOUDI: Okay. No further questions. Thank you.

THE COURT: All right. Can Mr. Fisk be allowed to escape?

MR. FRIEDMAN: Almost, Your Honor.

REDIRECT EXAMINATION

BY MR. FRIEDMAN:

Q. You were just asked a question about how Ms. Thompson ultimately accessed the data?

A. Yes.

Q. And would you take a look at Exhibit 108? Does that reflect how she actually accessed the data?

A. Yes.

Q. How is that that she did that?

A. So after stealing the credential, the role credential, she then used that directly to talk to the S3 service, not going through a Capital One service, and download the data from S3.

Q. So not -- over the AWS command line interface?

A. Right.

Q. The gateway into the data?

A. Yes.

MR. FRIEDMAN: Thank you.

And, Your Honor, we would actually offer Defense Exhibit 1013.

THE COURT: I agree. Let's put it into evidence. We've had enough conversation about the -- 1013, okay?

(Defense Exhibit 1013 admitted.)

MR. HAMOUDI: Thank you, Your Honor.

THE COURT: Yep. I'm not doing it because Mr. Friedman said so, I'm looking back to Mr. Hamoudi offering it and saying, yeah, why should we deny the jury the opportunity to see it.

So you'll see it and you can draw your own conclusions about what happened, okay?

MR. FRIEDMAN: No further questions, Your Honor.

THE COURT: Nothing else, Mr. Hamoudi?

MR. HAMOUDI: I just -- if we could publish 1013 for the jury to just look at for a moment.

THE COURT: But we do not need Mr. Fisk on the witness stand.

MR. HAMOUDI: No, we do not need Mr. Fisk on the witness stand.

THE COURT: Flee.

MR. HAMOUDI: Thank you, Mr. Fisk.

THE COURT: All right. And go ahead and publish 1013.
Just leave those there, we'll take care of them, thanks.

MR. HAMOUDI: I just learned it's not public, Your Honor, but I can put it on there.

THE COURT: Yeah.
Okay. That's good enough. Take a moment to look at it.
Okay. Everybody have a chance to look at it?
Great. Thank you.
All right. We have about 15 minutes, but shall we use it for the next witness?

MS. MANCA: Sure.

THE COURT: Great.

MS. MANCA: Your Honor, the government calls Zach Hansen from the FBI.

THE COURT: Agent Hansen, come on into the open area of the courtroom here and we'll swear you in.
Please raise your right hand.

ZACHAREY HANSEN,
having been first duly sworn, testified as follows:

THE CLERK: Please have a seat.
If you could please state your first and last names, and spell your last name for the record.

THE COURT: You can take your mask off if you want while you're testifying. It's totally up to you.

THE WITNESS: Thank you, sir.

Zacharey Hansen. Last name is H-a-n-s-e-n and first name is Z-a-c-h-a-r-e-y.

THE COURT: E-y, okay.

THE WITNESS: A-r-e-y.

THE COURT: Okay. Ms. Manca.

MS. MANCA: Thank you.

DIRECT EXAMINATION

BY MS. MANCA:

Q. Where do you work?

A. I work at the Seattle FBI; the FBI in Seattle.

Q. Okay. And what's your role within FBI?

A. I am a tactical specialist, which is a fancy way of saying a tactical intelligence analyst.

Q. And which divisions of the FBI do you support in that role?

A. Primarily, I support the Cyber Squad in Seattle.

Q. And what is a tactical specialist?

A. It's a fancy way of saying a tactical intelligence analyst. Primarily, I do desk work where I analyze or collect data in support of investigative activity conducted by agents that is primarily composed of doing open-source research, looking through databases that we already have information contained within, and analyzing data collected from legal process.

Q. What is open-source research?

A. Open-source research is accessing any data that is obtained from any sort of public space that anyone can freely access.

The best example would be from the Internet, such as going to Google and doing a search there.

Q. So does open source include areas of the Internet or social media that are protected by passwords or other privacy?

A. No. Open source would only apply to areas that anyone can freely access. So if there is some sort of password restriction, that's not open source anymore.

Q. What if looking into open source requires you to create an account in a certain social media like, say, Facebook?

A. If anyone is able to make an account freely at any time, then that is considered open source still, even if the information on the account is not accurate to who you are specifically.

Q. Okay. What are some of the procedures for if you want to create a fictitious account in order to access open-source information?

A. FBI has internal policy restrictions on when we can and cannot do that.

In this case, specifically, you have to have a certain standard to -- of the investigation has to have reached a certain point past the most basic, where we have an idea that there is some sort of activity going on, which means investigative activity, at which point I can create a fictitious online account, as we'd call it, an FOA, in order to conduct any sort of investigative activity online.

Q. How do you decide what name to use for your fictitious identity?

A. Generally, I try to go with popular enough names that it blends in fairly well. And I try not to use anything that would tie back to any real person.

Q. Did you create a fictitious identity for your investigation in this case?

A. Yes.

Q. What was the name that you used?

A. The primary name I used for most activity conducted here would have been Blanche Waller.

Q. How do you spell that?

A. B-l-a-n-c-h-e, and then last name would be W-a-l-l-e-r.

Q. And you conducted open-source research for this case; is that right?

A. That's true.

Q. And can you tell us what sites you reviewed in the course of your open-source research?

A. Many. The main ones I recall would be GitHub and GitLab, Twitter, Facebook, Meetup.com. I also viewed the Slack channel -- a Slack channel, I should say at this point. And those are the primary ones I recollect at this moment.

Q. I'm going to ask you about Twitter.

Can you tell me what Twitter account specifically you looked at?

A. I looked at -- the main Twitter account that came up in this account would be -- I don't remember the exact handle of the Twitter account, but it is something along the lines of OxA3A, and then it continues past there. It coincides with a PGP key hash that was provided to us from -- from Paige Thompson.

MS. MANCA: Okay. And, Agent, could you show Exhibit 437?

Q. (By Ms. Manca) Do you recognize that as the -- a tweet from the Twitter account that you're referring to?

A. Yes, I do.

Q. Okay. And what is the handle?

A. The handle is the word Erratic with the actual Twitter user name, being @OxA3A97B6C.

Q. And do you recognize this as one of the tweets that you reviewed?

A. It is.

Q. How did you document this open-source media as you were reviewing it?

A. I collected screenshots of any relevant items I found in open source, and then documented them into an FBI case file as a 1A in the case file.

Q. Do you -- and you recognize Exhibit 437 as one of your screenshots?

A. I do.

MS. MANCA: The government offers Exhibit 437.

THE COURT: Mr. Klein, any objection to 437?

MR. KLEIN: No objection, Your Honor.

THE COURT: 437 is admitted into evidence.

(Government Exhibit 437 admitted.)

MS. MANCA: And can we publish?

Q. (By Ms. Manca) And can you read -- well, for people who aren't familiar with Twitter, is this referred to as a retweet?

A. This is a response to a tweet. So in this case the user, Ryan Stalets, made a tweet in reply to another user, and the user Erratic responded to the tweet by Ryan Stalets.

Q. And what was her response?

A. Oh, if you only knew, friend, if you only knew.

Q. And what was the date of that tweet?

A. July 18th, 2019, it should be.

MS. MANCA: Okay. Okay. We can take that down.

Q. (By Ms. Manca) I'm going to ask you now some questions about Slack. I believe that you said that you reviewed Slack?

A. I did.

Q. Can you tell us what Slack is?

A. Slack is a messaging platform primarily used by businesses, but can be used by pretty much anyone who sets up a Slack server. And you can have group channels that you can have conversations on different topics, as well as it supports private messaging between users.

Q. And did you review a Slack channel related to Ms. Thompson?

A. I did. It was titled Netcrave.

Q. And how did you locate that Slack channel and connect it to Ms. Thompson?

A. When I was going through the open-source review for this case, one of the websites I came across was a Meetup.com event where the Netcrave Slack was linked to, by an account associated with Paige Thompson.

Q. And I previously reviewed with you Exhibits 402, 404, 406, 408, 410, 411, 413, 414, 416, 418, and 419. Did you recognize those as Slack communications that you reviewed?

A. If they're the ones that we reviewed together, then, yes, I reviewed all those.

Q. And are those screenshots that you personally took?

A. Yes.

Q. And do they fairly and accurately describe the contents of those Slack communications?

A. Yes.

MS. MANCA: Okay. Your Honor, we offer those exhibits that I just listed.

THE COURT: Counsel?

MR. KLEIN: Your Honor, I would object under foundation terms of when he took these screenshots and when he looked at them. They haven't clarified the timing of this. I would ask for some more information there for foundation.

THE COURT: All right. Ms. Manca, ask a little bit more about the foundation.

Q. (By Ms. Manca) So when you were looking through the Slack communication, can you tell me what date that would have been?

A. I can't say the specific date off the top of my head. It would have been recorded in the 1A, but it occurred approximately within the 10 days prior to the arrest around -- around late July.

Q. And as you looked at the Slack communications, how are you documenting what you look at?

A. So when I access the Slack channel, it allows you to go back prior to when you first joined and see historical messages that were included on the Slack channel.

And so when I went through, I read through them all, and I documented in screenshots containing some level of context, including my user name at the time and what channel I was in and what users were posting. I documented in screenshots any sections of chats which seemed relevant to the case at hand based on the information we had.

Q. Okay. And so those screenshots are simultaneous as you're reviewing the information online?

A. Could you rephrase that, please?

Q. The screenshots are -- you're taking them as you're reviewing the information?

A. Yes.

Q. And they fairly and accurately show what you're seeing on the screen?

MS. MANCA: Your Honor, once again, I offer those exhibits.

THE COURT: Yeah.

MR. KLEIN: No objection, Your Honor.

THE COURT: All right. I don't have the numbers right now, but if Victoria has them, we'll admit them all into evidence and you can display them.

(Government Exhibits 402, 404, 406, 408, 410, 411, 413, 414, 416, 418, and 419 admitted.)

MS. MANCA: Thank you.

And, Your Honor, we're going to address those, so that will allow us some time.

THE COURT: Okay. You're not going to -- you're just putting them in evidence right now.

MS. MANCA: That's correct.

THE COURT: Got it.

MS. MANCA: Thank you.

Q. (By Ms. Manca) The last genre of communications we're going to talk about is IRC chats. Are you familiar with that?

A. Yes.

Q. What is an IRC chat?

A. IRC stands for Internet Relay Chat.

Q. So it's probably not IRC chat, it's -- yeah.

A. And IRC is a platform. It's one of the older communication platforms for private messaging between individuals and group communication. It functions very similarly to Slack. Slack has an additional user interface added and some details are different, but IRC functions as a way for people to communicate individually with one another or in group chats that are set up based on topic or anything else somebody sets up.

Q. And did you review Internet Relay Chats in this case?

A. I did.

Q. And where did you find the Internet Relay Chats that you reviewed?

A. Those ones were provided to me via a collection obtained after -- during the search.

And then our forensic team collected information off of the devices that were obtained during the search and provided me with the chats for review.

Q. Okay. So can you identify who within the FBI specifically provided you the chats that you reviewed?

A. Computer scientist Waymon Ho provided me with the copies that were collected.

Q. And what was the format in which you reviewed them?

A. I reviewed a directory system that mirrored what was found on the -- as a working copy of the originals, and the log files that were inside of them contained the chats. The log files were reviewed with a Notepad-like program called Notepad++.

Q. And have you reviewed related to this case Exhibits 450 through 462?

A. If those are the ones we reviewed together which contain the IRC communications, then, yes.

Q. Okay. Are these fair and accurate copies of IRC chats that you reviewed that were provided to you by Waymon Ho?

A. Yes.

MS. MANCA: Your Honor, we offer Exhibits 450 to 462.

MR. KLEIN: One second, Your Honor, just looking through.

THE COURT: Okay.

MR. KLEIN: Your Honor?

THE COURT: Yes.

MR. KLEIN: We don't have an objection, but there may be some rule of completeness issues to raise on cross.

THE COURT: Okay. Thanks.

450 through 462 are admitted into evidence.

(Government Exhibits 450-462 admitted.)

MS. MANCA: Thank you, Your Honor.

May we publish Exhibit 450?

THE COURT: Sure.

Q. (By Ms. Manca) So, Mr. Hansen, each of these exhibits has a few pages, and I'm taking an example, Exhibit 450. What are we seeing on the first page of this exhibit?

A. On this exhibit, this is the log file within context as I viewed it, which I paired when I provided this with a screenshot showing the actual contents of log files that were obtained that were deemed relevant. And you can see in the top bar that is the directory for the computer and the beginning -- the beginning part of the file path, where it says IRC chats from 1B52, that is FBI's internal evidentiary location for this. And then later on when you start to get to the references to Z and C mod data log, these are all subdirectories of one another that mimic what was on the device that was imaged at the search location, which contain different chat logs that were on Paige Thompson's device.

Q. And what about this number 2019-04-05, what does that relate to?

A. That is the date of the log file that it was -- that it is from. And you can see where it was obtained from or what chat it was obtained from as well by looking in the URL bar.

In this case, it would be a communication with a user using the name Rachel that was -- occurred on 2019-04-05 as the date.

Q. Okay. Thank you.

And I am actually going to provide some context with Slack.

MS. MANCA: Agent, can you put up Exhibit 402?

Q. (By Ms. Manca) Okay. And would you mind zooming up on that upper right-hand corner? Or, I'm sorry, upper left-hand, left and right, tough.

Is that the name that you were using to access the Slack channel?

A. Yes, it is.

Q. Okay. And then what kinds of screen names are we going to see in the Slack communications when we address these with other witnesses?

A. Screen names I recall that were used by -- that appear to be used by Paige Thompson in this case would be Paige Adele, Paige Adele Thompson, Erratic, Sucky-sucky, and those are the ones that I can recall at the moment. I do believe there are others that I don't recall.

(Off the record.)

MS. MANCA: No further questions. Thank you, Mr. Hansen.

THE COURT: Okay. So, Agent, could you be back, please, at 1:15?

THE WITNESS: Sure.

THE COURT: And we'll do cross-examination then.

We'll take our lunch break now.

As I indicated, I have a judges' meeting that I want to get to that starts at noon, so leave your pads and pens on your chair.

We'll be reporting to Judge Pechman's courtroom, please, at 1:15, and we'll get started about 1:20, okay?

Great.

THE CLERK: Please rise.

(Court in recess 11:58 a.m. to 1:21 p.m.)

THE FOLLOWING PROCEEDINGS WERE HELD
IN THE PRESENCE OF THE JURY:

THE COURT: We'll continue with the now cross-examination of Agent Hansen. You're still under oath.

CROSS-EXAMINATION

BY MR. KLEIN:

Q. Good afternoon.

A. Good afternoon.

Q. So you do open-source research for the FBI?

A. That is one aspect of my job, yes.

Q. So one part of your job is to do open-source research?

A. Yes.

Q. And as part of that, do you use common search engines, like Google?

A. I use common search engines like Google, and then a number of tools and resources online.

Q. Do you ever use data from network scanners, like Shodan?

A. I have in the past, but not as typically as one might think, and not in this case.

Q. But you have used data from network scanners in the past?

A. I've used data from Shodan specifically.

Q. Any other network scanners?

A. Not that I recall.

Q. And do you ever find things, when you do your open-source research, things that are -- that someone has posted publicly that surprise you?

A. Could you rephrase that?

Q. Sure.

Do you ever find things, when you're doing your open-source research, that you're surprised that someone would choose to post publicly?

A. I have learned that people post a lot of stuff online. I'm not so surprised by most things anymore online.

Q. So people do post some crazy stuff online?

A. People do post a wide range of things online, yes.

Q. I want to talk to you for a moment about GitHub.

Do you know what GitHub is?

A. Yes.

Q. What is it?

A. GitHub is a website used by people to post excerpts or whole sections of code in order to, very often, share in public repoze, is what they're called, repositories, or sometimes in private ones or ones dedicated to certain groups.

Many companies keep their own sections that they can share between them, and many individual users will keep their own accounts, where they can contribute to different groups of code or can write stuff themselves for their own projects.

Q. So this is a well-respected place for people to post code or different engineering types of projects?

A. GitHub is well known, well respected.

Q. Microsoft owns it?

A. Yes, Microsoft does own it.

Q. When did you access Ms. Thompson's gists?

A. That would have been sometime in the ten days prior to the arrest.

Q. And how did you access them?

A. With the Internet, on a computer.

Is there something more specific?

Q. Did you have to use a password?

A. No.

Q. You were just able, through your open-source public research, to access her gists?

A. The initial links to the gist that Paige Thompson had were a link that was not -- I should step back here.

When you make a repository on GitHub, you can make it public and you can make it private. Paige Thompson's GitHub was publicly accessible. She may have had some stuff that was private that I could not access or see, but there is another type of data, which is unlisted, which means that you're able to access it if you have a link to it, and anyone can access this link and view the information at it.

The stuff I viewed on Paige Thompson's GitHub were unlisted items and public items, but I was not able to see any private data that was posted by Paige Thompson.

Q. You're only aware of data you saw, correct?

A. Yes.

Q. And so you saw stuff that was either publicly posted or for which you had a link you could access?

A. Yes.

Q. As part of open-source research, you're aware that people use -- do you know what a "handle" is?

A. Yes.

Q. What is a handle?

A. A handle is another name for a user name, a moniker that you go by.

Q. And do people use handles often that are not their own name, like something that's funny or interesting or descriptive?

A. I've rarely have seen somebody use their own name as a handle, except in a business or a professional setting.

Q. Okay. Let's talk for a moment about the tweets that you found.

A. Okay.

Q. When did you access Ms. Thompson's Twitter account?

A. Sometime within the ten days prior to the arrest.

Q. And her Twitter account was public?

A. Yes, it was, or at least any resources that I contributed that I affirmed were all public.

Q. So the exhibits that you talk about, that were shown by the prosecutor, those were publicly available?

A. Yes.

Q. And that means anyone in the public can view them; you don't have to have a Twitter account, even, right?

A. Yes.

Q. So you chose the name Blanche Waller, right?

A. Blanche Waller, that I used specifically on Slack.

Q. And for this case?

A. For this case -- I used Blache Waller on Slack. I don't recall all the -- if I used any other specific user names for Twitter. I don't believe I even made an account. But this was also three years ago, but I don't believe I made one for Twitter.

Q. Okay. But it was a name you chose to disguise the fact that you're with the FBI?

A. Blanche Waller? Yes.

Q. And let's talk about Ms. Thompson's Slack or the Netcrave group you talked about, right?

A. Yes.

Q. Called NetCrave, I think, her Slack channel?

A. Netcrave Communications, I believe, was the name of the Slack channel.

Q. And when did you access that, again?

A. Sometime within ten days prior to the arrest.

Q. And so before her arrest, you accessed her Slack or Netcrave. How did you access it?

A. I accessed it via a link that was posted in order to go to the Slack channel for Netcrave Communications, and I had to create a name on there, which was Blanche Waller, and then that gave me access to the Slack.

Q. So that link was publicly available?

A. Yes.

Q. And then you just created a name and went on her Slack?

A. Yes.

Q. And that's where you found the exhibits the prosecutor talked to you about?

A. Yes.

Q. So your research included accessing -- and the exhibits we were all shown -- included her publicly available tweets, right?

A. Yes.

Q. And her publicly available Slack communications?

A. Yes.

Q. The IRC communications you were shown by the prosecutor?

A. Yeah.

Q. What is IRC, again?

A. IRC stands for Internet Relay Chat, and it is a form of communication, an instant-message system where you can create channels to communicate as groups, but usually based on topic of some sort, or you can have one-on-one instant messages.

Q. And this is used often by people?

A. Very widely. It's one of the earlier instant-message communication protocols.

Q. So it's an earlier version of a lot of things we use now, like Slack or other ways to communicate?

A. Yes.

Q. And was the IRC chats publicly available, too?

A. Not to my knowledge. It may have been, but I did not access those in a publicly available way. Those were --

Q. Were you aware that there was a bridge between the Slack and the IRC?

A. When I was reviewing the chats on one of the devices -- of the chat logs, there was an instance where -- and this was, I believe, in the IRC where Paige Thompson synced them, so someone posts from one directly into the other, but other than that, I was not aware of any direct connection between them.

Q. But there was a bridge between the Slack, which was publicly available, to the IRC that Ms. Thompson had posted?

A. You might have to define what you mean by "bridge" more for me.

Q. A link that could connect the two, so if you clicked on it, you could access the IRC.

A. I'm not aware of that existing. It could be there, but I have no knowledge of that specifically.

Q. So it could be there?

A. I don't know.

Q. Well, it could be. You don't know, but it could be, right?

THE COURT: Why would you ask somebody if it could be? Aren't we here for facts?

MR. KLEIN: We are, Your Honor.

THE COURT: If he doesn't know, he doesn't know.

MR. KLEIN: Yes, Your Honor. One more second here.

Thank you very much.

THE COURT: Okay. Thanks.

Any redirect?

MS. MANCA: I do, Your Honor.

THE COURT: All right. Ms. Manca?

REDIRECT EXAMINATION

BY MS. MANCA:

Q. When you reviewed IRC chats, were there different -- how -- were they all in one area of the computer, or were there different folders and files in the computer?

A. They are different folders and files. Some IRC chats, the logs were on the desktop device, and some of the logs were on the laptop device, and then when they fall into the subfolders, as seen in the exhibit shown earlier, there are different channels that are, like, different chat rooms, that each contain different logs that have different users in them. And then there are also individual one-on-one communications as well. And these are contained, in this case, at least across two different devices that I reviewed.

Q. And did you see the hashtag Netcrave channel as one of the many channels that you reviewed?

A. Yes, I did.

Q. You mentioned, in your direct testimony, that Ms. Thompson used both the screen names Paige Adele and Erratic?

A. Yes.

Q. Did you see both of those names in the open-source material that you reviewed on Slack?

A. Yes, I did.

Q. Do you know how a user would rotate between those screen names within one Slack channel?

A. So in Slack, it is possible to change your user names. In this case, one of the connections to the Slack channel was in the -- across the totality of open-source information that I reviewed associated with Paige Thompson, I saw these user names, which provided -- and connected to accounts that provided a link to the Slack channel as well.

MS. MANCA: No further questions. Thank you.

THE COURT: Anything else, Mr. Klein?

MR. KLEIN: Nothing further, Your Honor.

THE COURT: Thank you very much. You're excused. Thanks so much for coming in.

And the government's next witness is Agent Martini?

MR. FRIEDMAN: Yes, Your Honor.

THE COURT: Agent, please come forward. You know the routine. You've seen it many times.

JOEL MARTINI,
having been first duly sworn, testified as follows:

THE CLERK: Please state your full name for the record, and spell your full name for the court reporter.

THE WITNESS: Joel Martini; last name, M-a-r-t-i-n-i.

THE COURT: Go ahead, Mr. Friedman.

MR. FRIEDMAN: Thank you, Your Honor.

DIRECT EXAMINATION

BY MR. FRIEDMAN:

Q. Good afternoon, Special Agent.

A. Good afternoon.

Q. Where do you work?

A. I work for the FBI.

Q. And I think the title gave it away, but what is your job at the FBI?

A. I am a special agent.

Q. What does a special agent do?

A. A special agent is just an investigator.

Q. How long have you been a special agent at the FBI?

A. I've been an agent for about five years now.

Q. What did you do before that?

A. Before that, I was also with the FBI, but I was working as a computer forensic examiner, so that just means I analyzed digital data.

Q. Are you assigned to a particular squad at the FBI?

A. I am.

Q. To what squad are you assigned?

A. I'm on the Cyber Squad.

Q. What does the Cyber Squad do?

A. Cyber Squad investigates high-technology crimes; that can be computer hacking or things that involve computers generally.

Q. Are you the case agent for this case, the investigation of Paige Thompson?

A. I am.

Q. What does a case agent do?

A. The case agent, I would liken to the quarterback of the team. So, obviously, there is a lot of people that are involved in an investigation, but the case agent kind of just tries to organize and make sure that everything is moving forward.

THE COURT: I'm just thinking the quarterback gets blamed if the team loses, too.

Q. (By Mr. Friedman) When did law enforcement first open what became this case?

A. I opened this case on July 22nd of 2019.

Q. That was a Monday?

A. It was.

Q. Were you the first person in law enforcement to receive information about this, or had it bounced somewhere first?

A. No. My understanding is that our FBI office in New York got the initial information just a couple of days before that.

Q. Over the weekend?

A. Correct.

Q. And then was the case referred to Seattle?

A. It was.

Q. And you were assigned as the case agent?

A. Yes.

Q. How serious or how high priority a case was it when it came into your office?

A. It was very -- it was top priority at the time.

Q. Okay. And why is that?

A. Because our understanding, based on the information that we received initially, was there was a lot of PII, or personal identifying information, that was at risk, and we wanted to do everything we could to mitigate that potentially being disseminated or being further disseminated, and just close that loop as fast as we could.

Q. Did that affect how the rest of your week went?

A. It did.

Q. Did you form a plan of what the goal was?

A. The goal was to be able to identify where the data was, who may be responsible, and then action that as fast as we possibly could.

Q. And what steps did you take during those first few days to identify the things you wanted to identify?

A. We did everything, from interviews to the open-source research that was discussed, as well as eventually initiating some surveillance; just trying to use as much of the toolbox that we possible could throughout that week.

Q. And did you learn additional information through that investigation?

A. We did.

Q. And did you form an action plan?

A. Yes. We obtained a search warrant on Friday of that week.

Q. For what was that search warrant?

A. The search warrant was a residential search warrant for a house down in south -- south of Seattle.

Q. Is four to five days from getting a case to having a search warrant quick or slow for your squad?

A. It was pretty unprecedented to go from no case to search warrant in about four days.

Q. When was that search warrant executed?

A. We executed that on the 29th of July, so exactly one week after opening.

Q. And were you one of the people who participated in executing that warrant?

A. Yes.

Q. Where did you execute that warrant?

A. As I said, it was a residence down in South Seattle.

Q. Would you take look at Exhibit 301 and tell me if you recognize that?

A. I do.

Q. What is that?

A. This is the front door of the residence we searched that day.

MR. FRIEDMAN: The government offers Exhibit 301.

MR. HAMOUDI: No objection.

THE COURT: 301 is admitted.

(Government Exhibit 301 admitted.)

Q. (By Mr. Friedman) Who lived at that residence?

A. There was a number of people, to include Paige Thompson.

Q. When agents arrived at the house, what did they do?

A. As is our standard practice, we clear the residence for safety; make sure there is nothing in there that's going to hurt anyone, and that includes taking the residents of the house outside of the house while we do that so that we can secure everything before we begin the search.

Q. Okay. After you had taken the residents outside of the house, were they in the neighborhood? In the yard? Where were they?

A. Yes, they were right in front of house.

Q. And then did agents begin searching the house?

A. Yes.

Q. Would you take a look at Exhibit 302 and tell me if you recognize that?
A. I do.
Q. What is that?
A. This is a sketch that was made of the residence.
MR. FRIEDMAN: The government offers Exhibit 302.
MR. HAMOUDI: No objection.
THE COURT: 302 is admitted.
(Government Exhibit 302 admitted.)
Q. (By Mr. Friedman) Can you tell us, in general, what this sketch shows?
A. The sketch just shows the different rooms in the house, primarily. There's a living room; that's Room A, for example. And Room C would be Paige Thompson's bedroom.
Q. And would you take a look at Exhibit 303 and tell me if you recognize that?
A. I do.
Q. What is that?
A. That's Room A, or that living room.
MR. FRIEDMAN: Government offers Exhibit 303.
MR. HAMOUDI: No objection.
THE COURT: 303 is admitted.
(Government Exhibit 303 admitted.)
Q. (By Mr. Friedman) And would you also look at Exhibit 304 and tell me if you recognize that?

A. Yes. That's the Room C that I just referenced.

Q. Paige Thompson's room?

A. Correct.

MR. FRIEDMAN: Government offers Exhibit 304.

MR. HAMOUDI: No objection.

THE COURT: 304 is admitted.

(Government Exhibit 304 admitted.)

Q. (By Mr. Friedman) Would you take a look at Exhibit 305 and tell me if you recognize that?

A. I do.

Q. What is that?

A. So this is a computer that we found, as you can see, right inside the door of that Room C.

MR. FRIEDMAN: Government offers Exhibit 305.

MR. HAMOUDI: No objection.

THE COURT: 305 is admitted.

(Government Exhibit 305 admitted.)

Q. (By Mr. Friedman) Would you describe for the jury what you're calling "the computer"?

A. Yes. The large box, if you will, that's kind of propped there behind the door that has the blue cable running out of it, that is a pretty large custom-built computer.

Q. And if you could look at Exhibit 306.

A. Yes. This is a photo of that same computer, the back side of that computer.

MR. FRIEDMAN: Government offers Exhibit 306.

MR. HAMOUDI: No objection.

THE COURT: 306 is admitted.

(Government Exhibit 306 admitted.)

Q. (By Mr. Friedman) In what state was the computer when you found it?

A. It was in Seattle, so that would be Washington State.

Q. Sorry. Wrong question.

Was the computer on or off?

THE COURT: That's being literal. I like it.

A. My mistake. It was on.

Q. (By Mr. Friedman) And so what did you and others -- and/or others do when you found that computer?

A. The first thing we typically do is perform a RAM capture. So that is just creating a copy of the running memory that's on the computer so that we don't lose that.

And then we do a cursory review of the computer, because we don't know what's going to happen with it over time, so we want to capture as much as we can right off the bat.

Q. Did you observe anything on the computer that was happening?

A. I did.

Q. What did you see?

A. We found a mounted folder that was named "aws_dumps."

Q. Did you have an understanding of what "aws" meant?

A. Yes. I understood that to mean "Amazon Web Services."

Q. And what about the word "dumps"?

A. That typically means files that have been downloaded, or copies.

Q. Would you take a look at Exhibit 408 and tell me if you recognize that?

A. I do.

Q. And what is Exhibit 408?

A. This is a screenshot from the Netcrave Slack channel that we discussed, and this particular highlighted portion shows, basically, a directory file listing of various files that are in a specific folder.

Q. Okay. And did those relate to what you saw on the computer?

A. Yes, they did match.

Q. And how is that? I think you just answered.

A. The files here were the same files that we found in that aws_dumps folder.

Q. Would take a look at Exhibit 308 and tell me if you recognize that?

A. I do.

Q. What is that?

A. It is a laptop that we found in that same room.

MR. FRIEDMAN: Government offers Exhibit 308.

MR. HAMOUDI: No objection.

THE COURT: 308 is admitted.

(Government Exhibit 308 admitted.)

Q. (By Mr. Friedman) And would you look at Exhibit 309 and tell me if you recognize that?

A. Yes. This is an iPhone cell phone also found in that same room.

MR. FRIEDMAN: Government offers Exhibit 309.

MR. HAMOUDI: No objection.

THE COURT: 309 is admitted.

(Government Exhibit 309 admitted.)

Q. (By Mr. Friedman) The phone is a little northwest of the picture?

A. Yes.

Q. Does the FBI have a system that it uses to track evidence that it seizes during search warrants?

A. Yes.

Q. In general terms, what is that system?

A. It's just a cataloging system that gives unique numbers to each evidence item so they can be tracked.

Q. What's the first number, usually?

A. One.

Q. Is it a little more complicated than one? I mean, are there several digits?

A. Our naming convention is 1B for these type of items. So it would be 1B-1 for the first item, and then so on.

Q. Do you recall what number was assigned to the large computer found in this room?

A. I believe it was 1B-56.

Q. Could it be 1B-2?

A. 1B-2 would be the laptop.

Q. And then what number was assigned to the iPhone?

A. 1B-3.

Q. And then would you take a look at Exhibit 310 -- it is a three-page exhibit -- and tell me if you recognize that?

A. I do.

Q. What is that?

A. These appear to be e-gift card receipts. So you can go online and get a gift card that is -- not a -- not physical gift card, but one you can spend online.

MR. FRIEDMAN: Government offers Exhibit 310.

MR. HAMOUDI: No objection.

THE COURT: 310 admitted.

(Government Exhibit 310 admitted.)

Q. (By Mr. Friedman) Special Agent Martini, what does the first page of Exhibit 310 show?

A. This first page just shows two copies of what appear to be two $100 e-gift cards.

Q. One copy of two gift cards?

A. Yes, correct.

Q. And then what's on the second page?

A. Just more of the same.

Q. And then the third page has one more?

A. Just another one, yes.

Q. So did the FBI find a total of five of those gift cards?

A. Yes.

MR. FRIEDMAN: May I have a moment, Your Honor?

THE COURT: Sure. Take a moment.

Q. (By Mr. Friedman) Special Agent Martini, would you also look at Exhibit 307?

A. Yes.

Q. Do you recognize that?

A. Yes. This is a photograph, just taken from a standard camera, of the screen of that large computer that we saw behind the door, and this is the aws_dumps folder.

MR. FRIEDMAN: Government offers Exhibit 307.

MR. HAMOUDI: No objection.

THE COURT: 307 is admitted.

(Government Exhibit 307 admitted.)

Q. (By Mr. Friedman) Where do you see the folder name on this exhibit?

A. At the very top, you can see "aws_dumps."

Q. And then you said this matched data you had seen somewhere else?

A. Right. If you compare these file names in the running lists, they match the one that was uploaded to Slack.

Q. Okay. And from what you've learned since the investigation, what do those files represent?

A. These are archived copies of data that was taken from Amazon Web Services accounts.

Q. Okay. And is each file a particular unit or division? How does that work?

A. For the most part, each one of these files is a different entity or different account, but there are some that appear to be related, such as Apperian and Apperian 2.

Q. Thank you.

Was Ms. Thompson interviewed on the morning of July 29th?

A. Yes.

Q. Was she advised of her Miranda rights before that interview?

A. Yes.

Q. And what are Miranda right?

A. Miranda rights are things that you -- you may be familiar with your right to remain silent. There's several of those rights. But they're what we provide to anyone that we're -- before we're conducting a custodial interview.

Q. Were those provided orally, or in writing?

A. Yes, actually, both. So we ask somebody that we're interviewing to sign a piece of paper that has all those rights written on it, but we also go over it verbally.

Q. And did Ms. Thompson subsequently indicate that she wanted to speak with agents?

A. Yes.

Q. So who participated in interviewing Ms. Thompson?

A. It was primarily myself and Zach Hansen, who we just heard from.

Q. At the beginning of the interview, did you ask Ms. Thompson questions about iPredator and TOR?

A. I did.

Q. And what did Ms. Thompson respond?

A. She originally stated that she did not use either of those services.

Q. And based upon evidence you knew at the time, did you believe that to be true or false?

A. I believed that to be false.

Q. And what evidence led you to believe that was false?

A. The postings and communications that we'd already reviewed.

Q. Would you look at Exhibit 406? Do you recognize that?

A. Yes. This is a Netcrave Communications post, and, as you can see, it does reference iPredators as well as TOR.

Q. And where do you see that reference?

A. Right in the middle there where it states, "I'm like iPredator and then TOR and then S3."

Q. Did Ms. Thompson say anything about the scanning tool?

A. She did.

Q. What did she say?

A. She said that she had developed a scanning tool specific for Amazon Web Services that was designed to look for misconfigurations and be able to hit the Instance Metadata Service.

Q. Did she use the word "misconfigurations" or "misconfigured"?

A. I believe so.

Q. Did Ms. Thompson say whether she had downloaded information from any of those servers?

A. She said she didn't remember if she had downloaded any such information.

Q. Was that consistent with other evidence you had already seen at that time?

A. It was not consistent, no.

Q. Why do you say that?

A. Again, just based on the postings that we had previously reviewed.

Q. And would you look at Exhibit 203, the third page?

A. Yes.

Q. Is that one of those postings?

A. Yes.

Q. And what do you see there that's inconsistent with what Ms. Thompson told you?

A. Just the three terabytes of S3 buckets indicates to me that there was downloading happening.

Q. Did Ms. Thompson say what had happened to any data that she might have downloaded?

A. She originally stated that she had not -- not looked at any data, even if it had been downloaded.

Q. Did she say anything about whether she had deleted any data?

A. She did say that if there had been data that was downloaded, it probably was deleted as well.

Q. Did you believe that the statement that data had been deleted was true or false, based on what you knew at the time?

A. I believed that to be false.

Q. And why is that?

A. Again, statements that had been made, but also, just shortly before that, we had found aws_dumps folder on the computer.

Q. As the interview progressed, did Ms. Thompson change what she said about some of these subjects?

A. Yes.

Q. And, specifically, did she change what she said about iPredator and TOR?

A. Yes.

Q. What did she say later on about those?

A. Later on, she said that she did actually use those services.

Q. Did she say for what she used the services?

A. I don't recall.

Q. Did Ms. Thompson say anything about downloading Capital One data?

A. She said that she had downloaded Capital One data, yes.

Q. Did Ms. Thompson correct her earlier statement about looking or not looking at the data?

A. No.

Q. Sorry. My question was complicated.

What was the earlier statement?

A. She -- she -- I'm sorry. Can you rephrase?

Q. What was the first statement about looking at data?

A. Originally stated that she had not looked at any data that had been downloaded.

Q. And so did Ms. Thompson change that statement?

A. The statement was not changed.

Q. Did Ms. Thompson subsequently provide investigators with information about her computer?

A. Yes.

Q. What did she provide?

A. She provided us with a password, as well as an encryption key for the computer, as well as a cell phone.

Q. Did Ms. Thompson say anything about who she had told or not told about her activity?

A. She stated that she had talked about the vulnerability or the issue with one former Amazon co-worker.

Q. Did she identify that co-worker?

A. She did.

A. What did she say?

A. Simply, that she had had a conversation with this individual.

Q. Oh, but did she provide a name for that individual?

A. Oh, yes.

Q. What was that name?

A. Robert Long.

Q. Did Ms. Thompson say anything about having tried to report this vulnerability to anyone?

A. No.

Q. Did she say anything about having tried to report it to any of the companies whose data she had downloaded?

A. No.

Q. After the day of the search, did you serve search warrants on a number of companies to gather records in this case?

A. I did.

Q. Was one of those companies GitHub?

A. Yes.

Q. And would you take a look at Exhibits 251 and 252 -- I guess I should say have you looked at Exhibits 251 and 252 in preparation?

A. I have.

Q. Were those documents that you obtained from GitHub?

A. Yes.

MR. FRIEDMAN: Government offers Exhibits 251 and 252.

MR. HAMOUDI: No objection.

THE COURT: 251 and 252 are admitted.

(Government Exhibits 251 and 252 admitted.)

Q. (By Mr. Friedman) So we're about to look at Exhibit 251, Special Agent. What is Exhibit 251?

A. This is kind of the identifiers of the GitHub account.

Q. Is it subscriber information?

A. Yes, that's fair.

Q. Whose account was this?

A. Paige Adele Thompson's.

Q. And you see that in the top line, I take it?

A. Yes.

Q. And would you take a look at Exhibit 252? This is another document you received from GitHub?

A. Yes.

Q. For this account?

A. Yes.

Q. What is this document?

A. This is a copy of something we've already seen before, the April 21st file, or a specific post that was made to that account.

Q. Okay. Special Agent Martini, did you also serve a search warrant on Slack?

A. Yes.

Q. Were you seeking records relating to a particular account or channel there?

A. Yes, the Netcrave channel that we've discussed.

Q. And did you obtain records from Slack in response to that?

A. Yes.

Q. I think I said "subpoena," but I assume it was a search warrant.

A. It was a search warrant, yes.

Q. Are Exhibits 401, 403, 405, 407, 409, 412, 415, 417 and 420 all part of the records you received from Slack?

A. Yes.

MR. FRIEDMAN: The government offers that list of exhibits.

MR. HAMOUDI: No objection.

THE COURT: Those exhibits are admitted into evidence.

(Government Exhibits 401, 403, 405, 407, 409,
412, 415, 417 and 420 admitted.)

Q. (By Mr. Friedman) Let's look at Exhibit 401. What is it?

A. It is a subscriber record for the Slack channel.

Q. And who does this show was the subscriber or owner of that channel?

A. Paige Thompson.

Q. And then if we could turn to Exhibit 409 --

MR. FRIEDMAN: Oh, I'll wait a moment.

Q. (By Mr. Friedman) Special Agent, where do you see a subscriber on these records?

A. There's several places, but the one that I'm immediately drawn to is the real name, which says "Paige Thompson."

Q. Okay. And then if we could turn to Exhibit 409. What is Exhibit 409?

A. It's a listing of those same file names that we've seen several other places.

Q. The ones that were on the computer screen during the search?

A. That's right.

Q. And previously posted on Slack?

A. That's right.

Q. Would you take a look at Exhibit 413 and tell me if you recognize that?

A. I do.

Q. What is Exhibit 413?

A. More communications from the Netcrave channel.

Q. And if we could highlight, perhaps, the bottom three posts. Would you read the long sentence in the middle of the bottom post?

A. The one that begins, "I mean"?

Q. The one right below that that begins, "It's weird."

A. "It's weird what the world has come to and yet despite how important security is for some, I can still log in to so much with admin/admin."

Q. Do you have an understanding of what logging into something with admin/admin means?

A. Yes. Admin/admin is often a default user name and password for a lot of things. So logging into admin/admin would indicate to me that you're just trying default credentials in order to hope that somebody hasn't changed them, and you can get in to something.

Q. I assume you do some sophisticated cases?

A. Yes.

Q. Do you see cases where the hack is -- the owner had not changed the password, and someone hacked in by typing "admin/admin"?

A. Absolutely.

Q. Is there anything in this series of posts or tweets where Ms. Thompson suggests that's actually authorized?

A. No.

MR. HAMOUDI: I object to that last answer, Your Honor.

THE COURT: Well, the exhibit speaks for itself, so I'll sustain the objection.

Q. (By Mr. Friedman) Did you also obtain records from Twitter?

A. Yes.

Q. Did you serve a search warrant on Twitter to gather those?

A. I did.

Q. Are Exhibits 431, 433, 434, 435, 436, 438, and 439 part of the records you received from Twitter?

A. Yes.

MR. FRIEDMAN: The government offers that list of exhibits.

MR. HAMOUDI: No objection.

THE COURT: That list of exhibits is admitted.

(Government Exhibits 431, 433, 434,
435, 436, 438 and 439 admitted.)

Q. (By Mr. Friedman) If we can look at Exhibit 431. What is Exhibit 431?

A. The subscriber information for the Twitter account.

Q. Do you see something called a screen name there?

A. Yes.

Q. What is a screen name?

A. Screen name is the handle or identifier for the account.

Q. Okay. Is that a screen name that you've seen previously in this case?

A. It is.

Q. Where have you seen that?

A. That was one of the -- that was the Twitter account that we looked at through open source.

Q. And do you see an email address for the subscriber?

A. Yes.

Q. What is that email address?

A. paigeadele2019@gmail.com.

Q. Do you know, from your investigation, to whom that email account, the paigeadele2019 account, belongs?

A. Yes. We obtained Google records that tied that to Paige Thompson as well.

Q. Do you see an account number for this Twitter account?

A. I do.

Q. And is an easy way to refer to that just the last four digits of that account?

A. Sure.

Q. What are the last four digits of that account?

A. 2768.

Q. Would you take a look at Exhibit 438 and tell me if you recognize that?

A. I do.

Q. That was a record you received from Twitter?

A. Yes.

Q. And what is that?

A. That is a copy -- a picture, rather, of the computer that we recovered in this case.

Q. And would you take a look at Exhibit 435?

A. Yes.

Q. What is Exhibit 435?

A. These are direct messages or private messages from that same Twitter account.

Q. When you say "direct message" or "private message," what does that mean?

A. Twitter has a function where you can DM or privately message somebody, and this is a copy of some of those messages.

Q. Okay. If we could zoom in on the fourth message, can you see who sent this message?

A. I can.

Q. And where do you see that?

A. If you see the field, "sender ID," it has that same number that we just talked about ending in 2768.

Q. So this was sent by the owner of this account?

A. That's right.

Q. And what does that message say?

A. It reads, "Yeah, this data that I stole, straight outta S3 because I'm just so incompetent, wouldn't have happened if this person had just left me alone."

Q. The reference to "straight outta S3," what do you understand that to mean?

A. Well, it says, "stole straight outta S3," so I believe that to mean that data was exfiltrated or taken out of S3, which is the Amazon storage solution.

Q. And did you see an explanation here of what Ms. Thompson's motive was for doing that?

MR. HAMOUDI: Objection as to motive. This exhibit speaks for itself.

MR. FRIEDMAN: I can go on, Your Honor.

THE COURT: Okay. Go ahead.

Q. (By Mr. Friedman) Would you look at the first message on this page? Is that also sent by the owner of this account?

A. Yes.

Q. Does that say what Ms. Thompson intends to do with this information?

A. It appears to, yes.

Q. What does it say?

A. It says, "I'm gonna give it to worse people, too. I'm gonna give it to an avid scammer, a Chinaman who will find a good permanent home for it on the black market, sealed with a story behind it."

Q. Special Agent Martini, did you also obtain records from Google in response to a search warrant?

A. Yes.

Q. Are Exhibits 521 through 525 some of the records that you obtained from Google?

A. Yes.

Q. And, in general, to how many different accounts do those records apply?

A. Several.

Q. Okay. Do you recall the names of those email accounts, or would it be helpful to look at the records?

A. It would be helpful.

Q. If we could look at Exhibit 521, can you tell what this account is?

A. This is subscriber information for one of the accounts. As you can see here, the email address for the records here is paigeadele@gmail.com, but you can also see a recovery email down below with paige.adele.thompson@gmail.com.

Q. What is a recovery email?

A. It's a way, if you lose your password to your account, you can have a recovery email associated with it so that that email address can have an email sent to it with a recovery token or password so you can get back into your original account.

Q. Okay. If we could look at Exhibit 523, for what email account were these records?

A. This one is for paige.adele.thompson@gmail.com.

Q. That's the recovery address on the last account we looked at?

A. Yes.

Q. And if we can look at Exhibit 525?

A. Yeah, this one is for paigeadele2019@gmail.

Q. Did you conclude that all three of these accounts were accounts belonging to Ms. Thompson?

A. Yes, we were able to connect all of them.

Q. And if we could go back to Exhibit 521, do you see a nickname at the top of the subscriber information that connects this to other accounts that you'd seen in this case?

A. Are you referring to the nickname "Erratic"?

Q. Yes.

A. Yes.

Q. Have you seen that elsewhere in the case?

A. Yes.

Q. Did the records also include something called "Internet history"?

A. Yes.

Q. If we can look at Exhibit 522?

MR. FRIEDMAN: I apologize, Your Honor. I have not offered Exhibits 521 to 525, so I'd offer them now.

THE COURT: Any objection?

MR. HAMOUDI: No, Your Honor.

THE COURT: 521 to 525 are admitted.

(Government Exhibits 521 to 525 admitted.)

Q. (By Mr. Friedman) Special Agent, let's not go back through the other subscriber records, but on 521, this account, can you just show us where you see the subscriber's name, email, and nickname?

A. Sure. At the top, you see the name, "Paige Thompson," email, "paigeadele@gmail," and then towards the bottom there, the nickname "Erratic," as well as a recovery email, paige.adele.thompson@gmail.com, kind of in the middle of the screen.

Q. Thank you.

And if we could go to Exhibit 522, is this the first page of an Internet history for one of these accounts?

A. Yes.

Q. What is Internet history?

A. Internet history is just a running list of places that you visited on the Internet. So if you use Google, for example, it keeps track of the web pages that you go to, and this is a listing of what those would be.

Q. Does it also show what you did at some of those pages?

A. It can.

Q. In this case, does it?

A. It -- yeah, it -- well, it -- this one -- it shows things that you've searched for, and gives you recommendations as well.

Q. Okay. Special Agent Martini, you heard testimony from Zacharey Hansen a few moments ago about something called Internet Relay Chat, or IRC?

A. Yes.

Q. Have you reviewed the IRCs in this case?

A. I have.

Q. If you will look at Exhibit 453, the second page, do you see discussion here about data that Ms. Thompson had taken from various entities in this case?

A. Yes.

Q. The first line, do you understand that to refer to a

particular company?
A. Yes.
Q. Which company is that, and why?
A. Well, the link is a GitHub gist, if that's what you're referring to.
Q. Yes. And is that a gist that you've seen before in this case?
A. I believe so.
Q. Which gist is that?
A. I believe this is the same gist that contains that April 21st Capital-One-related file.
Q. Okay. So do you understand this to be related to the Capital One data?
A. I do.
Q. As we go down through this, do you see a reference to a different company?
A. Yes.
Q. And I believe it's at 23:22:11. What does that line say?
A. Yes. On line 10, it says, "not nearly as good as that but Vodafone."
Q. And does Ms. Thompson explain how she had gotten data relating to Vodafone?
A. By -- according to line 12, it says, "by virtue of their payment gateway."
Q. And I should have asked you the question, the lead-in to,

"not nearly as good as that, but Vodafone"?

A. What line?

MR. HAMOUDI: Objection, Your Honor. I think these messages sort of speak for themselves. Mr. Martini was not present when these messages were entered. We don't know what was happening surrounding them. And if there is somebody present for these circumstances, they can offer that witness, but for him to sit there, on and on, I object.

THE COURT: It's like asking somebody, "could something have happened" when they didn't have anything to do with it.

MR. HAMOUDI: Yes.

THE COURT: Sustained.

MR. FRIEDMAN: Your Honor, I was going to ask what Mr. Martini did relating to this as the next question.

THE COURT: Okay. Ask that one first.

Q. (By Mr. Friedman) What did you do based on the references to Vodafone in this case?

A. We contacted them about them potentially being part of this case.

Q. What is Vodafone?

A. It is a telecommunications conglomerate out of the United Kingdom.

Q. And what data does Ms. Thompson say he or she has of Vodafone's?

A. Line 14 references that she has their certs.

Q. Do you have an understanding of what a cert is?

A. My understanding, in this context, is they are certificates, which potentially could be used to access --

MR. HAMOUDI: I object, Your Honor.

THE COURT: Well, it's his understanding, so I'll --

MR. HAMOUDI: But I would --

THE COURT: -- let him finish. Go ahead.

A. My understanding is they are certificates that may be used to access other data.

Q. (By Mr. Friedman) Did you see a reference to Vodafone in another IRC?

A. Yes.

Q. If we could look at page 2 of 462.

What does Ms. Thompson say about Vodafone data here?

A. Well, on line 9, it says, "I've got a mirror of all their S3 buckets," referring to Vodafone, which is in line 8.

Q. And what is a mirror?

A. "A mirror" is a common word to refer to a full copy.

Q. And does Ms. Thompson say anything about her possession of that data in the following line?

A. The following line reads, "How am I not" --

MR. HAMOUDI: Same objection.

THE COURT: Aren't you going to ask him about this, too?

MR. HAMOUDI: Well, I don't think so, Your Honor.

THE COURT: Okay. If you're not going to, then the exhibit speaks for itself.

MR. FRIEDMAN: Yes, Your Honor.

Q. (By Mr. Friedman) Did Ms. Thompson say what she intended to do with some of this data in another IRC?

A. Yes.

Q. Would you take a look at Exhibit 454, page 2, and if you'd look at the line 21.

A. Okay.

Q. What does Ms. Thompson say she's going to do with certain data?

A. This appears to be a message to another user. It says that -- it says, "makes me want to leak these TSA S3 buckets."

Q. Do you have an understanding of what "TSA" means in this context?

A. Yes. The folks at the airport.

Q. Transportation Security Administration?

A. That's right.

Q. And have you seen TSA data in this case?

A. Yes, we recovered it from one of the archives.

Q. From which archive did you recover that?

A. It was called Apperian.

Q. Special Agent Martini, did you look at the cell phone that was seized from Ms. Thompson's residence?

A. I did.

Q. Were you the primary person who did that?

A. Yes.

MR. FRIEDMAN: Your Honor, at this point, we have a stipulation that we'd like to read, with the agreement of the defense, or I could hand it to the Court, if the Court would rather.

THE COURT: No. You can read it, as long as Mr. Hamoudi is okay with it.

MR. HAMOUDI: No objection.

MR. FRIEDMAN: Your Honor, the parties stipulate or agree to the following:

"No. 1, the FBI seized an Apple iPhone Model A1905, and iPhone 8, from Paige Thompson's bedroom on July 29th of 2019, and assigned the item Evidence No. 1B-3.

"No. 2, John Powers works for the FBI analyzing cellular telephones. Using forensic software, Powers processed the Apple iPhone 8, 1B-3, and provided a true and correct image of the phone's contents to FBI Special Agent Joel Martini for his review.

"The parties stipulate and agree that no further testimony is necessary to prove that the image of Evidence No. 1B-3 that Special Agent Martini received is a true and correct image of what was recovered from a phone seized by the FBI from Ms. Thompson's bedroom.

"To be clear, this stipulation means only that the image is an accurate representation of the phone's contents. There is no agreement as to the truth of the content of any statements in Evidence No. 1B-3, or the weight to be given them.

"This stipulation shall be read to the jury in lieu of having a witness testify as to the source and validity of the exhibit, and may then be admitted into evidence and provided to the jury."

THE COURT: Does the stipulation have an exhibit number now?

MR. FRIEDMAN: It does not, but we will provide one and file it that way, Your Honor.

THE COURT: And it will be admitted into evidence.

And when the parties stipulate to certain facts, you should treat those facts as established when you decide the case. Okay?

Q. (By Mr. Friedman) Special Agent Martini, how did you examine that cell phone?

A. I examined it with common forensic software.

Q. And what does that forensic software allow you to do, in general terms?

A. Essentially, it takes a copy of the phone and parses it. It creates little buckets, if you will. So for web history, for contacts, for phone calls, it just puts everything in a nice, little specific area so you can navigate it better.

Q. Are Exhibits 501 through 506 some of the data that you seized from the cell phone?

A. Yes.

MR. FRIEDMAN: The government offers Exhibits 501 through 506 into evidence.

THE COURT: 501 through 506 are admitted.

(Government Exhibits 501 through 506 admitted.)

Q. (By Mr. Friedman) Special Agent Martini, would you look at Exhibit 501? What are the items shown on this page?

A. These are text messages, or SMS, from the phone.

Q. What does the first one say?

A. "I, however, hijacked more aws accounts."

Q. And if we could go down to the bottom messages -- I apologize. We should go to the next page, page 2, please.

Do you see one message on that page?

A. Yes.

Q. Could you read, starting halfway through the second sentence of that message, and just through the word "overlooked" from there, would you read that out loud?

A. From the word "overlooked"?

Q. Beginning "I have," and then down to "overlooked." So "I have" in the middle of the second line.

A. "I have my own dilemmas, as you well know. Actually, I'm not so sure you do. Try having root IAM credentials for some pretty large companies in your pocket because some minor thing was overlooked."

Q. Are you able to see the phone number of the phone that sent this message?

A. Yes.

Q. And where is that phone number?

A. It appears to be right above the message.

Q. And what is that phone number?

A. In this case, it is area code (206) 602-9923.

Q. Did you see anything in any of the text messages that you seized in which Ms. Thompson stated that companies had given her permission to take this data?

A. No.

Q. Did the information that you obtained from the phone also include Internet history?

A. It did.

Q. And would you look at Exhibit 504 and tell me if you recognize that?

MS. MANCA: I'm sorry?

MR. FRIEDMAN: 504.

MS. MANCA: We're going to have to come back to that one. I'm sorry.

Q. (By Mr. Friedman) Special Agent Martini, did you review the Internet history on the phone?

A. I did.

Q. Did you read all of it?

A. Yes.

Q. I don't have any specific questions for you about it, but let's look at Exhibit 506.

I see the words "extraction report" up top, and then "autofill" is the next word?

A. That's right.

Q. What is autofill?

A. Autofill is a feature that you find on a lot of digital devices. If you get tired of filling in your name or your address, you know, as you're constantly going to different websites or signing up for things, you can have your browser or the tool remember what that is so it just automatically puts it in, you don't have to keep retyping.

Q. Is that why, if you're not careful, autofill sometimes puts someone other than you intended?

A. It can.

Q. Where do phones get the data they use to autofill?

A. You have to enter it at some point and tell the device to save that data.

Q. Do you tell the device to save the data, or can the device do it by itself?

A. I suppose both are technically possible.

Q. What is this autofill document?

A. It is a list of information that appears to have been saved in the autofill feature.

Q. If we look at lines 3, 4, 5, and 6, what do you see there as being saved?

A. A user name, but, specifically, "Joseph Baleda."

Q. Does that suggest that this name was entered once or more than once, or can you not tell that?

A. It's hard to tell.

Q. Can you tell anything from this about the purpose for which that name was entered?

MR. HAMOUDI: I'm going to object to that.

THE COURT: Well, just a "yes" or "no" answer.

A. No.

Q. (By Mr. Friedman) And then under the "Joseph Baleda," do you see a slight variant on that for two more lines?

A. Yes.

Q. And what is that variant?

A. Joseph.Baleda.

Q. Okay. And can you tell for what purpose that was entered into the phone?

A. No.

Q. Below that, what do you see? What are the next two entries?

A. Another iteration that appears to be of the same name, "Joey Baleda."

Q. I'm sorry. I meant the two entries above that.

A. Oh, I'm sorry.

Yes, it's an answer autofill with the entry "pizza."

Q. And then two more of "Joey Baleda"?

A. Yes.

Q. What do you mean by an "answer autofill"?

A. Just to differentiate from user name, which is how the Joseph Baleda, Joseph.Baleda, and Joey Baleda are tagged.

Q. Does that suggest the word "pizza" was entered as an answer to something?

A. That's right, a different type of field, yes.

Q. As opposed to name and someone entered "pizza," in which we'd see user name "pizza"?

A. Yes.

Q. And then we see "DOB day." What do you see there?

A. Yes, the answer to that is -- the saved answer to that is "21."

Q. And down further to the bottom half of the page, do you see several answers to "DOB year"?

A. Yes.

Q. And what do you see there?

A. The entry "1991."

Q. Okay? Do you see -- three and four lines from the bottom, do you see autofill answers for an email address?

A. Yes.

Q. What do you see there?

A. Entries for the email address josephbaleda@mailinator.com.

MR. FRIEDMAN: May I have a moment, Your Honor?

THE COURT: Sure.

MR. FRIEDMAN: Thank you.

Q. (By Mr. Friedman) And then if we could go to the second page of this document, do you see an autofill for "DOB month"?

A. I do.

Q. And what is that?

A. The entry of "10."

Q. So between these three things, we've had a DOB for day, month, and year?

A. Yes.

Q. Have you put those together in your mind?

A. Yes.

Q. And what day and month and year do those add up to?

A. It would be October -- I'm sorry, I don't remember the day -- of 1991.

Q. Okay. Let's go back to the previous page.

A. Twenty-first.

Q. Okay. So October 21st, 1991?

A. Yes.

Q. Are you aware of an individual named Joseph Baleda who has a connection to this case?

A. Yes.

Q. Are you aware of his birthday?

A. Yes.

Q. What is his birthday? Is it the date you just said?

A. October 21st, 1991.

Q. Do you see a mailing address listed here?

A. I do.

Q. What is that mailing address?

A. 901 Dexter Avenue North.

Q. And do you see a phone number autofilled in three increments?

A. Yes.

Q. What is that phone number?

A. It appears to be area (425), with a prefix 882, and the suffix 8080.

Q. Let's go back to the previous page for a minute, if we can, and at the bottom, the third and fourth lines from the bottom.

You talked a moment ago about the email josephbaleda@mailinator.com.

Are you familiar with something called Mailinator?

A. Yes. Mailinator is an anonymous email service, one that's designed to be disposable.

Q. Okay. Is Mailinator a service provider from which law enforcement can obtain records?

A. Not that I'm aware of, no.

Q. Did you try or inquire?

A. Yes, yes.

Q. Were you able to obtain any records?

A. No records.

Q. Based on what you see on this, can you tell any purpose for which the name Joseph Baleda was used?

MR. HAMOUDI: Objection.

THE COURT: Just a "yes" or "no."

A. No.

Q. (By Mr. Friedman) Okay. You see the data here, but you can't say for what it was used?

A. That's right. The data was entered, but I don't know ultimately for what purpose.

Q. Okay. Special Agent Martini, you've been talking about the cell phone that you examined. Are you aware of the phone number that was associated with this cell phone?

A. I believe it was the one that was listed at the beginning of the text messages that we had observed.

MR. FRIEDMAN: May I have one moment, Your Honor?

THE COURT: Sure.

Q. (By Mr. Friedman) Special Agent Martini, I assume -- did you look through all of the available data on this phone --

A. I did.

Q. -- that you were authorized to?

A. I did.

Q. Did you see any evidence that anyone other than Paige Thompson was a user of this phone?

A. No.

Q. Special Agent Martini, have you worked with some of the companies whose data was taken during the course of your investigation of this case?

A. Many of them, yes.

Q. Have you provided them any information to help their investigation or things they need to do?

A. Many of them, yes.

Q. And why is that?

A. It's important that the companies understand how they were impacted, so whatever we can do, whatever we can share, based on the information that we've come into possession of, especially in things like the aws_dumps folder, we want to share that back to the company so that they can mitigate it appropriately.

Q. Did you provide each company all of the data taken, or did you sometimes provide more limited information?

MR. HAMOUDI: Objection; relevance.

THE COURT: It's interesting. Go ahead. You can answer.

A. It was kind of a tiered process, so we'd often provide them with limited information at first, in order for them to verify that it was, indeed, their data, and then we'd often follow that up with a more full copy of the information.

Q. (By Mr. Friedman) Was one of the companies to which you provided information a company named Apperian, or later, Digital.ai?

A. Yes.

Q. And are Exhibits 720 and 721 data or information that you provided to Apperian?

A. Yes.

MR. FRIEDMAN: The government offers Exhibits 720 and 721.

MR. HAMOUDI: I'm going to object. I'd like to hear from the Apperian people, if they're going to testify.

THE COURT: Well, this question is did he provide it to them.

MR. HAMOUDI: Yeah, that's fine, Your Honor.

THE COURT: So the objection is withdrawn. You answered the question "yes"?

THE WITNESS: Yes.

Q. (By Mr. Friedman) Did you provide information to other companies from which data had been taken?

A. Yes.

Q. And did those include 42Lines, a company that was once named Survox and is now Enghouse, a company named Bitglass, and Vodafone?

A. All of those, yes.

Q. And are Exhibits 730, 731, 740, 741, 750, 751, 752 and 760 data that you provided, in each case, to one of those companies?

A. That's right.

MR. FRIEDMAN: Government offers that list of exhibits.

MR. HAMOUDI: Objection; subject to the same.

THE COURT: Okay. I'll take that up outside -- you're not going to ask him about the data, are you?

MR. FRIEDMAN: Only in one case, Your Honor. In the other case, it's too late for basis of witnesses who will testify.

THE COURT: I'll take it under advisement, but you can ask him about the one you want to ask him about.

Q. (By Mr. Friedman) Special Agent Martini, did you look at data that you found in folders that had suggested it had been taken from Vodafone?

A. Yes.

Q. And did you look inside that data?

A. Yes.

Q. Can you describe, generally, the volume of data that had been taken from Vodafone?

A. I believe the archive was roughly about 17 gigabytes in size. It was pretty large.

Q. And what type of data did you see in there when you looked?

A. There was a variety of information, but files that indicated that they were some sort of --

MR. HAMOUDI: Objection, Your Honor, as to content.

THE COURT: Overruled. You can answer.

A. Files that indicated that they were some sort of certificate type of file.

Q. (By Mr. Friedman) And why did you consider that significant?

A. It matched what we understood the Vodafone data to be.

Q. And from where did you get your understanding of what the Vodafone data was?

A. Vodafone themselves.

MR. HAMOUDI: Objection; hearsay.

THE COURT: I think Mr. Friedman is asking about postings by Paige Thompson.

A. Yes, there were postings online that we observed that indicated that that's what it was.

Q. (By Mr. Friedman) Do you recall how Ms. Thompson had described that data in her posts?

A. As "certs," or certificates.

Q. And is that what you saw as part of the data that you examined?

A. That's right.

Q. Special Agent Martini, are you aware of an investigation that was opened by the Department of Justice?

A. In general terms, yes.

Q. Okay. And the U.S. Attorney's Office here is actually part of the Department of Justice, correct?

A. That's right.

Q. Is this a different part that we're talking about?

A. Yes.

Q. And, specifically, what part?

A. My understanding is it's Main Justice, so back East.

Q. Did you have an understanding -- I'll show you Exhibit 952. Did you have an understanding about what was the subject of that investigation?

A. Yeah. My understanding is that investigation centered around this note.

Q. Did you have an understanding of how extensive that investigation was?

A. My understanding is there was --

MR. HAMOUDI: I object to this.

THE COURT: Yeah, I don't really know where this is going, so I'd rather hear about it outside the presence of the jury.

MR. FRIEDMAN: That's fine, Your Honor.

THE COURT: And since Agent Martini is here, we can always recall him.

MR. FRIEDMAN: Would you like me to keep going?

THE COURT: In another area, yeah.

Q. (By Mr. Friedman) Special Agent Martini, have you reviewed Paige Thompson's entire Internet search history both from the computer and from the cell phone?

A. As much as we recovered, yes.

Q. Did you see information in there that related to credit card or possible credit card fraud?

A. Yes.

Q. And would you take a look at Exhibit 522, page 23?

Did you see information that related to cryptocurrency money?

A. I did.

Q. And would you take a look at Exhibit 524, page 2? Is that some of that information?

A. It is.

Q. And why do you say that?

A. These are visited web pages for Nanopool, which is a cryptocurrency pool, as well as the bottom -- or, rather, Nanopool endpoints, and the beginning of the Nanopool Ethereum web page.

Q. And what type of information did you see that related to credit card fraud?

A. A variety --

MR. HAMOUDI: Objection, Your Honor.

MR. FRIEDMAN: Your Honor, this would be --

THE COURT: Well, just an objection?

MR. HAMOUDI: Yeah, objection. These are questions in a way trying to extract.

THE COURT: The objection is overruled. You can answer. Go ahead.

A. Generally, things -- here we go.

Searches such as credit card number based on location, anatomy of a credit card, carding forums, dark web, marketplaces, things of that nature.

Q. (By Mr. Friedman) Did you see anything in either of the Internet search histories about responsible disclosure?

A. I did not.

Q. Did you see any searches for responsible disclosure websites?

A. I did not.

Q. Have you also looked at Ms. Thompson's social media communications, messagings, postings?

A. Yes.

Q. Did you see either of those things -- did you see communications about responsible disclosure in any of those?

A. Not that I observed.

MR. FRIEDMAN: Thank you. I have no further questions.

THE COURT: How's everybody doing? Can you go a little longer without a break?

Okay. Mr. Hamoudi, we'll do cross-examination of Agent Martini.

CROSS-EXAMINATION

BY MR. HAMOUDI:

Q. When you looked at Ms. Thompson's web searches, you found 17,000 web searches, correct?

A. There was many, yes.

Q. And a lot of the web searches were over a matter of seconds or minutes, correct?

A. I don't know the exact time frames.

Q. The exhibits speak for themselves. Can we bring some of them up? 506. So let's look at the time period of this.

A. Sure.

Q. This Chrome fill. Up top, please, it's March 28 at 2:58 a.m., right?

A. That's right.

Q. And then let's go down to the bottom to the -- it looks like 2:54 a.m.?

A. That's right.

Q. But you don't know the circumstances of what's going on when a human being is in front of a device and what they're doing, correct?

A. I don't.

Q. And you don't know what their mental state is?

A. No.

Q. You don't know whether if they're on medication?

A. No.

Q. You don't know if they're not feeling well?

A. No.

Q. And you did testify, I believe it was in June of 2021, before a grand jury; do you recall that?

A. That sounds right, yes.

Q. Yes?

A. Yes.

Q. And a grand juror asked you a very direct question. They asked you a question about if the data in this case was used by anybody else. Do you remember that?

A. Generally, yes.

Q. I can bring up the transcript.

A. Yeah, if you have it, please.

Q. Yeah, I can bring it up.

I can't bring it up, but do you recall being asked by a grand juror if the data in this case was being used by anybody else?

A. Not specifically.

MR. HAMOUDI: Go to 82. All right. We can't find it.

THE COURT: I'll take a break, if it would make it easier for you.

MR. HAMOUDI: It would.

THE COURT: Victoria will take you downstairs, and we'll get started again, really promptly, please, at five of 3:00, because at 3:45, we're going to break early because I have a swearing-in of the magistrate judge.

Please go down to Judge Pechman's courtroom, and we'll bring you back at five of.

THE FOLLOWING PROCEEDINGS WERE HELD
OUTSIDE THE PRESENCE OF THE JURY:

MS. MANCA: Your Honor, can we address the scheduling matter?

THE COURT: We can do it now, yes.

MS. MANCA: I don't know how much longer we have with Agent Martini. We have one more very brief witness. And then our next witness, if we started with a new witness this afternoon, would be a very lengthy witness. So our preference would be to break this afternoon after the witness that's coming after Agent Martini, and that way we can start with our out-of-town witnesses early in the morning tomorrow.

THE COURT: That's fine to do it that way.

Why don't we put the quick witness up now, if you don't mind just interrupting.

MR. HAMOUDI: I don't mind, Your Honor.

THE COURT: Because he's going to be here.

MS. MANCA: That's fine. I think we can get them both.

THE COURT: We don't know how long Mr. Hamoudi is going to be on cross.

MS. MANCA: I'm worried about the situation --

THE COURT: If you get done, don't worry about it.

And while we're talking about scheduling things, Monday morning I need to start a little bit later, so we'll start at

10:30 on Monday, and we'll just kind of plow through things. But, sure, that's fine. Don't worry about that.

But if you want to get your other witness on, you know, we're all waiting with bated breath to get Ms. Culbertson to do something.

MS. MANCA: You will get that opportunity. I just didn't want to start with this really long witness right this afternoon.

THE COURT: We're adjourned until five of.

MR. FRIEDMAN: Your Honor, could we address, quickly, the question that the court had said we should put that off? Would you rather not do that?

THE COURT: Go ahead. We're back on the record.

MR. FRIEDMAN: I was just going to bring out, quickly, that there was this brief investigation at Main Justice. It was closed.

The defense made a big point about the OCC investigation and others, and so I was assuming that we're going to hear a lot about the Department of Justice conducted this investigation of Capital One.

THE COURT: What was DOJ investigating about the note?

MR. FRIEDMAN: We're not deeply privy to it, but they were focused on what Capital One -- this is the thing where we obtained 600 pages of discovery that were produced a few months ago --

THE COURT: Are you guys going to bring it up?

MR. HAMOUDI: No.

THE COURT: Let's just drop it.

MR. FRIEDMAN: Thank you.

THE COURT: And this was the old DOJ, right?

MR. FRIEDMAN: Well, the one in D.C., if that's -- yeah.

THE COURT: No. I mean, the Barr DOJ.

MR. FRIEDMAN: Yes.

(Court in recess 2:45 p.m. to 2:58 p.m.)

THE COURT: Please be seated. And we will continue with cross-examination of Agent Martini.

Q. (By Mr. Hamoudi) So, Agent Martini, you went through an extensive amount of evidence that you obtained as a result of search warrants you issued to variety of social media companies; correct?

A. That's right.

Q. GitLab, yes?

A. I don't remember if we did GitLab, but definitely GitHub.

Q. GitHub.

And Twitter?

A. Yes.

Q. Gmail?

A. Yes.

Q. And Netcrave?

A. Yes.

Q. And Google?

A. Google's included, yes.

Q. Yes.

And then -- and you did a thorough search of all of that evidence; correct?

A. That's right.

Q. And there's no evidence that Ms. Thompson ever shared Capital One's data with anyone; correct?

A. Not that I found.

Q. And no evidence that she shared anyone's data with anyone; correct?

A. Not that I found.

Q. Okay. No evidence that she ever sold it; correct?

A. Not that I found.

Q. Publicly disclosed it?

A. Not that I found.

Q. Any evidence that she tried to blackmail anyone?

A. Not that I found.

Q. No evidence that she ever leaked any of the data?

A. No.

Q. Okay. And we were talking about web histories.

MR. HAMOUDI: And let's go to 522-03, please. It's previously admitted.

Q. (By Mr. Hamoudi) Isn't it true that only four Google searches related to credit card fraud?

A. I believe there was more than just this one page.

Q. Okay. Which page is it on?

A. I don't know off the top of my head.

Q. Okay. Isn't it true that all of these searches that you testified to occurred within a 30-minute time span?

A. Approximately, that appears true.

Q. And her search history revealed no downloads of embossers or actually visiting any of these credit card web forums, do they?

A. Not that I recall.

Q. Okay.

And I want to go back to the circumstances of the search warrant.

A. Sure.

Q. So just for educational purposes, a search warrant is -- it gives you permission to go somewhere; correct?

A. That's right.

Q. And without a search warrant, you can't -- you don't have permission to go to that place; correct?

A. In a law enforcement capacity, exactly.

Q. Right.

So before you could go to Ms. Thompson's home or where she was living, you had to go to a judge and you had to get permission to go over there; correct?

A. That's right.

Q. And so you went and obtained this warrant. And the warrant gave you authority to seize items at the residence; correct?

A. That's right.

Q. And the warrant was fairly broad, it allowed you to seize all computers, notebook computers, laptop computers, electronic storage media, and components; correct?

A. Yes.

MR. HAMOUDI: And can you bring up discovery 551?

Q. (By Mr. Hamoudi) And subsection 12B, one of the provisions that gave you authority to seize items, can you read that out loud?

A. 12B, you said?

Q. Yes.

A. Yes.

Any digital devices or other electronic storage media used to facilitate the transmission, creation, display, encoding, or storage of data, including word processing equipment, modems, docking stations, monitors, cameras, printers, plotters, encryption devisors -- sorry, encryption devices, and optical scanners.

Q. And then so when you executed the search warrant at Ms. Thompson's residence, there were surveillance cameras that were destroyed by the FBI; correct?

A. I believe that is true.

Q. And that was to prevent the tactical -- so somebody knows the tactics that you use to execute a search warrant?

A. That's right.

Q. All right. But if we take the warrant at its terms, it didn't give you permission to destroy the cameras; correct?

A. I -- I mean, based on this, I don't see anything having to do with destroy. But I would also say that there's a difference between the data storage and the camera itself. I mean, the camera is just a camera that links to some other place.

Q. Well, it says cameras on there, correct, on 12B?

A. True, yes.

Q. Okay. So just by its written terms, you didn't have authority to destroy those cameras; correct?

A. Based -- it doesn't -- this specific 12B doesn't reference anything having to do with that.

Q. But the warrant gave you permission to be there, the warrant didn't give you permission to destroy things?

A. Based on this specific part of the warrant, that's true. But I don't know what else might be in the warrant.

Q. Okay. And when the search was executed -- there were roughly 30 to 40 agents when the search was executed; correct?

A. I don't know the exact number, but that's probably close.

Q. And there was a SWAT team used?

A. That's right.

Q. And they wore fatigues?

A. They did.

Q. And they were armed with assault rifles?

A. That's right.

Q. And they were armed with a battering ram?

A. I believe they had one, yes.

Q. Okay. And -- and so they started to bang and to get -- and what were they saying if -- what do you normally say when they're doing that?

THE COURT: Well, are -- you're assuming they're using the battering ram at the very beginning, so --

MR. HAMOUDI: Yes.

THE COURT: -- why don't you ask him whether they ever had to use it or they just --

Q. (By Mr. Hamoudi) Did they ever have to use the battering ram?

A. I wasn't there at that time, but I don't believe so.

Q. Okay. And then so --

THE COURT: You weren't part of the entry team?

THE WITNESS: I was not.

Q. (By Mr. Hamoudi) Okay. Ms. Thompson is -- agree, is a physically slight woman; correct?

A. Potentially.

Q. All right. You learned that her birth name was Trevor Thompson; right?

A. That's correct.

Q. And so you learned that she was transgender; correct?

A. Yes.

Q. And when -- and when --

MR. HAMOUDI: Can you bring up Exhibit 304?

Q. (By Mr. Hamoudi) Do you recall what time of day -- do you recall when it was that the search warrant was executed?

A. I think it was approximately 6:00 in the morning.

Q. Okay. And you agree with me that here, this room, seems to be in quite a disarray?

A. Yes.

Q. Yeah.

And you did not seize items of significant value from this room, other than the computer; correct?

A. In accordance to the search warrant, that's right.

Q. All right. And you didn't see any designer clothes in the room, did you?

A. Not that I personally observed.

Q. No. Okay.

I want to talk to you about -- about the manner in which information was shared with you at the outset of the investigation by Capital One.

A. Okay.

Q. Okay. All right. You were involved -- you were not communicating directly with a Capital One employee, but you were speaking to lawyers that represented Capital One; correct?

A. For the most part, that's correct.

Q. And these lawyers were a New York-based law firm; correct?

A. That is my understanding.

Q. And so you relied on them to provide you information that you requested to inform your investigation; correct?

A. They originally provided us with a referral that had kind of a baseline. And then we went and independently verified as much as we possibly could from that referral.

Q. And at the same time, they were asking you for information in return; correct?

A. As we went forward, yes.

Q. Okay. So like in -- can you bring up 156-64.

And this is an email between yourself and an individual named Nicole Washburn. Do you see this?

A. Yes.

Q. And Ms. Washburn asks you that the OCC regulators asked today if the FBI would be providing us with a copy of their forensic report. And you responded that that -- you wouldn't -- you wouldn't normally do that; correct?

A. That's right.

Q. And you did say you would share some other information, which is a threat alert documentation based on your analysis to-date; correct?

A. That's right.

Q. And was that ever shared with Capital One?

A. I don't know off the top of my head.

Q. Okay. And I also saw that -- if you go down to the next page, you also assisted in getting them their data back; correct?

A. That's right.

Q. And she offhandedly makes a comment, I owe you a drink sometime. Do you see that down there?

A. I do.

Q. And is it normal for somebody to offer an FBI agent a drink sometime?

A. I don't know. I mean, that's not something that I guess we typically deal with or communicate about.

Q. And you're a trained professional, you know that you can't go have a drink with somebody --

A. That's right.

Q. -- right, but -- okay.

And you also -- I want to talk to you about the note that's been admitted.

MR. HAMOUDI: What exhibit is that?

(Off the record.)

Q. (By Mr. Hamoudi) 1100, when did you get a copy of this note?

A. I don't know off the top of my head, to be honest.

Q. You talked to Capital One's employees and a lot of times throughout this investigation; correct?

A. That's correct.

Q. And every time they talked to you, they had outside counsel present; correct?

A. That's correct.

Q. Okay. And at any time did they provide you this note?

A. We did eventually get a copy of this note, yes.

Q. Okay. And -- you don't know the date, though; correct?

A. I don't.

Q. Would January 24th, 2022 sound about right?

A. That's possible.

Q. Yeah.

MR. HAMOUDI: Why don't you bring up 141-55.

Q. (By Mr. Hamoudi) These are your handwritten notes?

A. They are.

Q. And it seems like this is an interview of Thomas Hall, says Tom. Do you know who he is?

A. I do. It would not have been an interview of him, although it may have been just a collective group of people.

Q. Okay. But this is the first time that the note is brought to your attention, do you believe?

A. Again, I don't know the exact date.

Q. Okay. But it wasn't provided to you early on in the investigation, was it?

A. I did not see it for quite some time --

Q. Okay. All right. How about let's go to 155-77?

THE COURT: So these numbers that Mr. Hamoudi is using are sort of Bates numbers on discovery. It has nothing to do with the trial. They're not exhibits or anything like that. And you won't be seeing them unless they're separately marked as exhibits and admitted into evidence.

Q. (By Mr. Hamoudi) So this is an example of you -- Nicole Washburn, she's sending you an email and she references the note. And she doesn't provide you the note; right? And Nicole Washburn also works for Capital One.

THE COURT: Well, there's like three questions in there.

MR. HAMOUDI: I apologize.

Q. (By Mr. Hamoudi) This is an email from Nicole Washburn; correct

A. It is.

Q. And she works for Capital One?

A. Yes.

Q. And she references the note, but then -- and you just ask what note/conference is that, do you recall?

A. Yes. I didn't have any context for that -- for the sentence.

Q. And she never followed up to then respond to that answer, your question you asked, what note/conference is that, she never followed up and provided you a response, did she?

A. Not to my recollection.

Q. And nobody -- none of the attorneys who represented Capital One ever followed up and provided you any information, did they?

A. Not to this email string.

Q. Okay. Thank you.

(Off the record.)

MR. HAMOUDI: Can you bring up 1002? But do not publish, please.

Go to the second page.

No, go to the first page.

Q. (By Mr. Hamoudi) Agent Martini, did Capital One ever provide you with a memorandum written by Rob Alexander to the Risk Committee, dated December 13th, 2019?

A. I personally don't believe I've seen this document.

Q. Okay. Go to the second page.

Did Capital One or its representatives ever tell you that the web access firewall role had been granted overly permissive access and the attacker was able to access our AWS storage from outside the Capital One network?

A. Sorry, can you point me to where that is?

Q. Yeah, B.

A. That does generally describe our understanding.

Q. Okay. But they never -- did they ever share this document with you in December -- after December of 2019?

A. Not with me personally.

Q. Okay. Okay. Thank you.

And you can take that down.

And were you -- were you aware -- I guess, what knowledge did you have about Capital One being investigated by the OCC, other than to request for the reports which Ms. Washburn had asked you?

A. It was completely separate from my investigation, so, limited.

Q. Okay. All right. All right.

(Off the record.)

Q. (By Mr. Hamoudi) Did you ever see trail logs, Amazon trail logs, for any of the companies in this case?

A. A handful of the companies did provide some of the trail logs, yes.

Q. Okay. And did you -- do you use TOR?

A. I've used it a couple times, more of an experiment, but that's about it.

Q. And you use a Virtual Private Network?

A. On occasion.

Q. And have you ever attended DEF CON?

A. I have not.

Q. No?

What is DEF CON?

A. DEF CON is a security information security hacking type of conference, usually held down in Las Vegas.

Q. Have you ever attended any other such conferences, hacking conferences?

A. Not specifically hacking conferences, no.

Q. Okay.

MR. HAMOUDI: No more questions, Your Honor.

THE COURT: How about Comic-Con?

THE WITNESS: Unfortunately, no.

THE COURT: That's the only one I know. I've never been there.

Mr. Friedman, any --

MR. FRIEDMAN: May I have a moment, Your Honor?

THE COURT: Sure.

(Off the record.)

MR. FRIEDMAN: No questions, Your Honor.

THE COURT: Okay. And so the defense is going to look at 720, 721, 730, 731, 740, 741, 750, through 752, and 760. Just let me know tomorrow, okay?

MR. HAMOUDI: Yes. I do have one small matter. The matter we addressed off the record, if Your Honor could just instruct the jury to disregard the initial information that was testified to.

THE COURT: About the investigation?

MR. HAMOUDI: Yes.

THE COURT: Yeah. You know, there was a reference to a DOJ investigation, and I said I'll take that up outside the presence. And both sides agreed they weren't going to go there.

So just ignore any of that testimony about DOJ investigation.

Thanks, Mr. Hamoudi.

MR. HAMOUDI: Thank you, Your Honor.

THE COURT: You can step down, Agent.

They evicted you from your chair, but Ms. Manca will give it back to you.

MS. MANCA: I will.

THE COURT: And the next witness of the day?

MS. CULBERTSON: Yes, Your Honor. The government calls Joseph Baleda.

THE COURT: So for those of you who are wondering what Ms. Culbertson was doing, now you know, she's going to do this witness.

Mr. Baleda, come into the well of the courtroom, which is this open area here.

And once you get a little bit closer -- please stop there.

Raise your right hand and my clerk will administer an oath to you.

JOSEPH ADAM BALEDA,
having been first duly sworn, testified as follows:

THE COURT: Have a seat up here, Mr. Baleda.

And if you want to take -- leave your mask on, that's fine. If you want to take it off while you're answering questions, that's what most people have been doing, so it's totally up to you.

THE CLERK: If you could please state your first and last names, and spell your last name for the record.

THE WITNESS: Joseph Adam Baleda. It's B-a-l-e-d-a.

THE COURT: Okay. So you pronounce it Baleda.

THE WITNESS: Yes.

THE COURT: Great. Thank you.

Go ahead, Ms. Culbertson.

MS. CULBERTSON: Good afternoon Mr. Baleda.

DIRECT EXAMINATION

BY MS. CULBERTSON:

Q. Where do you currently live?

A. Detroit, Michigan.

Q. And what you do you for a living?

A. I'm a 3-D artist.

Q. Any particular kind of 3-D artist?

A. Environment art for games.

Q. Okay. By "games," do you mean video games?

A. Yes.

Q. Where were you living in 2019?

A. In Seattle.

Q. Have you ever applied for a Capital One credit card?

A. Yes.

Q. Do you remember about when that might have been?

A. Like later -- late 2019.

Q. Okay. Is there a possibility it might have been in early

2019?

A. Yeah, early, late --

Q. Sometime in 2019?

A. -- sometime in 2019.

Q. Okay. Do you remember if your application was approved?

A. Yes.

Q. Okay. And do you still have an account with Capital One?

A. Yes.

Q. How did you first learn that you were involved in this case?

A. I was reached out to by Special Agent Joel Martini.

Q. Was that a phone call from Special Agent Martini?

A. Yes.

Q. And what did you learn on that phone call?

A. That some of my data had been stolen from me and, uhm, some of my information had been compromised.

Q. Okay. And do you know if -- where that information came from that was compromised?

A. From -- from what I understand, a Capital One breach.

Q. Capital One breach, okay.

Do you have any reason to think that your credit has been impacted by your information being taken from Capital One?

A. Not that I'm aware of.

MS. CULBERTSON: Your Honor, I'm planning to show Mr. Baleda a document that's been marked as Exhibit 782. It's a document that we're going to offer through our computer scientist, Mr. Waymon Ho. It's a document that he found on the defendant's computer. But may I provisionally offer it now, show it to the jury, and ask this witness to answer questions about it?

THE COURT: I don't know what it is just yet, so don't show it to the jury just yet, but show it to him and me.

MS. CULBERTSON: Special agent, if you can call up Exhibit 782.

(Off the record.)

MS. CULBERTSON: There we go.

THE COURT: So, Mr. Hamoudi, do you have an objection to this exhibit?

MR. KLEIN: Your Honor, I do object to foundation. I don't think this witness has ever seen this document.

THE COURT: No, he hasn't. And they're not offering it through him, but to -- they're going to ask him to identify something on there.

Do you have a problem with it later --

MR. KLEIN: I guess I don't have a problem with limited questions, Your Honor, but, from what I know, this isn't a document he's ever seen before.

THE COURT: Yeah, drop the questions, she's going to ask the questions, the question is, do you have a problem showing it to the jury right now?

MR. KLEIN: I don't, Your Honor.

THE COURT: Okay. So we're not admitting it just yet, but it's going to come -- if it comes in, it will be through Mr. Ho's testimony, but Mr. Baleda will have a chance to just see what's there and tell you.

Go ahead, Counsel.

MS. CULBERTSON: Great.

And if you could go ahead and publish that document to the jury.

Q. (By Ms. Culbertson) Mr. Baleda, I'm showing you a document that has been marked as Exhibit 782. Are you able to see that?

A. Yes.

Q. Do you see that -- this part that's blown up, sort of it looks like two portions of content, there's a line break between the first and the second portion. Do you see that?

A. Yes.

Q. Okay. The first part of the document, does that look like some kind of printout of data?

A. Yes.

Q. Okay. And then there's a line break and the second part has an email address, some words and a phone number. Do you see that?

A. Yes.

Q. Okay. Looking at the top part of the document, do you see your name in there?

A. Yes, I do.

Q. Also, in that top part of the document, do you see a Dexter Avenue address there?

A. Yes.

Q. Do you recognize that address?

A. Yes. That's the address I was living at when I applied for the Capital One account.

Q. When you were living in Seattle?

A. Yes.

Q. Okay. And again, still in that top part of the information, do you see an email address joeybaleda@gmail.com?

A. I see a gmail.com. Some of the document has been blurred out for me.

Q. Has been redacted, okay.

Do you see in the top part of that document the words "lastFourSSN," followed by a blacked-out --

A. Yes.

Q. -- gray square?

Okay. Still in this top portion, do you see a date of birth on here?

A. I do.

Q. Okay. Can you tell me the year of the date of birth that you see?

A. 1991.

Q. Okay. And Mr. Baleda, can you tell me what your birthday

is?
A. October 21st, 1991.
Q. Okay. Turning now to the information in the bottom portion of this document, do you see an email address on there?
A. Yes.
Q. What is that email address?
A. Josephbaleda@mailinator.com.
Q. Is that an email address that you set up?
A. No.
Q. Have you ever used that email address?
A. No.
Q. Do you then see under that email address "crakka442C"?
A. Yes.
Q. Is that a phrase that means anything to you?
A. No. I'm unfamiliar with this.
Q. Is it a phrase that you've ever used as a password?
A. No.
Q. Is it a phrase that you've ever used as the answer to a security question?
A. I don't believe so.
MR. KLEIN: Objection. He already said he was unfamiliar with it.
THE COURT: Right.
MS. CULBERTSON: I'll move on.
Q. (By Ms. Culbertson) Mr. Baleda, do you know Paige

Thompson, the defendant in this case?

A. No.

Q. Did you ever authorize Paige Thompson to open up a Mailinator account using your name?

A. No.

Q. Did you ever authorize Paige Thompson to use any of your personal information for any purpose?

A. No.

MS. CULBERTSON: Okay. Thank you.

THE COURT: Is your favorite food pizza?

THE WITNESS: I do like pizza.

THE COURT: Yeah, me, too.

All right. Go ahead, Mr. Klein.

MR. KLEIN: This will be quick.

CROSS-EXAMINATION

BY MR. KLEIN:

Q. Do you know if Ms. Thompson ever set up a Mailinator account in your name?

A. Not that I'm aware of.

MR. KLEIN: Nothing further, Your Honor.

THE COURT: So thank you very much for coming in. Hope you didn't get too nervous.

THE WITNESS: No.

THE COURT: Yeah. Good deal.

All right. You are excused. Thank you so much.

THE WITNESS: Thank you, Judge.

THE COURT: Okay. So I tell you, I've got this thing at -- where I got to get up there, so this is a good time for us to take a break in the action and let you get home a little bit early.

Please tomorrow, same time, 8:45, so we can get started promptly at 9:00. We'll put in a full day on Friday.

Monday, actually, we're going to start a little later, so you won't need to be here 'til about 10:15 on Monday morning, okay?

And stay healthy, stay well.

Don't do any research on the case.

We planted in your minds the idea that maybe you want to have pizza tonight and maybe a martini with it, and that's perfectly okay.

You are excused. Thank you so much.

THE FOLLOWING PROCEEDINGS WERE HELD
OUTSIDE THE PRESENCE OF THE JURY:

THE COURT: Okay. Thanks. Please be seated.

So I got an email from Mr. Klein saying, per the judge's request, here are the defense team cross-examiners for tomorrow, and for Joey Baleda it says Hamoudi.

MR. HAMOUDI: It was.

Your Honor, I'll tell you what happened.

THE COURT: Yeah. Oh, good, you're not going to make me guess. Thank you.

MR. HAMOUDI: I realized that I got Mike Fisk and Agent Martini, and then I had a son at home, and I got little overwhelmed. And I forgot to follow up and send the corrections. That's my responsibility. I apologize.

THE COURT: All right. And could we get tomorrow's.

MR. KLEIN: Yes, Your Honor. We will -- we're not exactly sure who they are, but we'll confer with the government and send you a list that will be dead-on right.

THE COURT: Okay. I mean, I totally -- it's okay to revise it, just let me know that you've revised it.

MR. KLEIN: We had forgotten it was later.

THE COURT: I mean, you asked one question, it's no big deal, it's just when you suddenly did an objection, I was like, why is he doing it rather than Mr. Hamoudi.

MR. KLEIN: Yes, Your Honor.

THE COURT: Okay. All right. So anything the government wants to bring to my attention about scheduling or anything?

MR. FRIEDMAN: No, Your Honor. Thank you.

THE COURT: Okay. So we'll see you tomorrow.

MR. KLEIN: Yes.

THE COURT: We're good.

All right. Start up again at 9:00 tomorrow. Thanks.

(Court adjourned at 3:29 p.m.)

CERTIFICATE

I, Nancy L. Bauer, CCR, RPR, Court Reporter for the United States District Court in the Western District of Washington at Seattle, do hereby certify that I was present in court during the foregoing matter and reported said proceedings stenographically.

I further certify that thereafter, I have caused said stenographic notes to be transcribed under my direction and that the foregoing pages are a true and accurate transcription to the best of my ability.

Dated this 9th day of June 2022.

/S/ Nancy L. Bauer

Nancy L. Bauer, CCR, RPR
Official Court Reporter